Joseph Fitsanakis

The Nerves of Government

Electronic Networking and Social Control in the Information Society

Submitted to the Faculty of Social Sciences of the University of Edinburgh, Scotland, in fulfilment of the requirements for the degree of Doctor of Philosophy

September 2001

Signed Declaration of Original Content.

In accordance with the University of Edinburgh's Regulations for Degrees by Research, §3.8.7 (a), (b) and (c).

I, Joseph Fitsanakis, hereby declare that the present thesis, entitled *The Nerves of Government: Electronic Networking and Social Control in the Information Society*, has been composed solely by me and therefore represents my own, original work. Additionally, no parts of this thesis have ever been submitted for any degree or professional qualification, except as specified.

Joseph Fitsanakis

PhD candidate
Department of Politics
The University of Edinburgh

Acknowledgements.

The contents of this volume are the outcome of a four-year effort which began in Edinburgh in October 1997. The experiences of these four years have taught me, among other things, that in the strictest sense, there is no such thing as "individual achievement". To the sceptical reader I offer this project as an appropriate illustration: it would not have been accomplished without generous amounts of critical assistance and support offered by many people and institutions. The least I can do in return is to thank them from this paper pulpit.

To begin with, I wish to thank the Science and Technology Unit of the University of Edinburgh for awarding me the three-year Economic and Social Research Council (ESRC) scholarship (Award no J00429734016) that made this project possible. My thanks also go out to the ESRC itself for its generous material assistance, including its Research Training Support Grant (RTSG), which financed 100 per cent of my research trips across the UK and the US.

This project was supervised by Charles D. Raab, Professor of Government at the School of Social and Political Studies at Edinburgh, and Professor Robin Williams, Director of the Graduate School for the Social Sciences, also at Edinburgh. Their supervision during these four years has been exemplary and their overall conduct aptly demonstrates how fruitful working relationships can be between graduate students and academic members of staff when both are committed to adherence to professional standards. Their numerous observations, recommendations and criticisms substantially enriched this project and were for me a valuable form of schooling, for which I am profoundly grateful.

Thanks are also due to Dr. Apostolos Georgiadis, Research Fellow at Edinburgh's Electrical Engineering Department, who patiently provided me with useful specialist knowledge and information on the micro-mechanics of digital and analogue communications interception.

During my interviews I gained useful insights into communications interception by speaking to knowledgeable professionals who are normally difficult to reach for purposes of research. I would have been unable to overcome such difficulties without crucial help from the following individuals: J.W., formerly of the UK's Special Branch; D.S., also of the Special Branch; D.Y., Special Agent with the FBI; I. L., an Emergency Communications professional in the US; Bobby Thompson, of BellSouth; and Sergeant E.K., a Communications Officer of the US Special Forces. My sincere thanks go out to all of them.

I have calculated that I travelled approximately 18,000 miles to facilitate this project's research schedule. Many people welcomed me in their homes during these trips, thus helping me to significantly reduce my accommodation bills and substitute faceless hotel rooms with the warmth and comfort of their homes. These remarkably generous people were the Parker family (Andy, Phyllis and Lisan) of Miami, Florida; the Thomas family (Clara, Joe and Lorie) of Bristol, Tennessee; my brother Minos, whose Derby apartment I turned into an 'interview operations centre' for a week in April, 2000'; and my good friends Harry Platanakis, of Edinburgh, and Nikos Kakalis and Myriam Conesa, also of Edinburgh.

Most of all, I want to thank my parents, George and Evie, who first taught me the importance of free thinking, and also my wife and friend, Vanessa, whose unmatched love and devotion sums up for me the meaning of all this.

Joseph Fitsanakis
Edinburgh, Scotland, 23 September 2001.

Table of Contents.

List of Abbreviations.

ACLU	American Civil Liberties Union
ACPO	Association of Chief Police Officers [UK]
AEB	Alliance for Electronic Business [UK]
AOL	America On Line [US]
AT&T	American Telephone and Telegraph [US]
ATIS	Alliance for Telecommunications Industry Solutions [US]
ATM	Asynchronous Transfer Mode
BILETA	British and Irish Law and Technology Association
BT	British Telecom, Ltd. [UK]
BTID	British Telecom Investigation Department [UK]
C3I	Command, Control, Communications and Intelligence
CALEA	Communications Assistance for Law Enforcement Act [US]
CEO	Chief Executive Officer
CI	communications interception
CIA	Central Intelligence Agency [US]
CID	Criminal Investigation Department [UK]
CLI	Calling Line Identifier
CND	Campaign for Nuclear Disarmament [UK]
CODEC	coder / de-coder
CP	Communist Party [of Britain]
CPSR	Computer Professionals for Social Responsibility [US]
CSE	Canadian Security Establishment
CSP	Communication service provider
CTIA	Cellular Telecommunications Industry Association
DATU	Direct Access Testing Unit
DCI	Director of Central Intelligence [US]
DIA	Denfence Intelligence Agency [US]
DNR	Dialled Number Recorder
DoD	Department of Defence [US]
DoJ	Department of Justice [US]
DORA	Defence of the Realm Act [UK]
DPA	Data Protection Act 1998 [UK]
DSE	Data Switching Exchange
DTI	Department of Trade and Industry [UK]
ECHR	European Convention on Human Rights
ECSPC	Electronic Communications Service Provider Committee [US]
EFF	Electronic Frontier Foundation [US]
EITC	Electric and International Telegraph Company [UK]
ESS	Electronic Switching System
ESTSFBI	Electronic Surveillance Technology Section of the Federal Bureau of Investigation [US]
FBI	Federal Bureau of Investigation [US]
FBICIS	Federal Bureau of Investigation CALEA Implementation Section [US]
FBITILU	Federal Bureau of Investigation Telecommunications Industry Liaison Unit
FCC	Federal Communications Commission [US]
FCS	Federation of Communications Services [UK]
FDM	Frequency Division Multiplexing
FEI	Federation of the Electronics Industry [UK]
FIPR	Foundation for Information Policy Research [UK]

FOIA	Freedom of Information Act [US]
FOUO	For Official Use Only [US]
FSB	Federal Security Service [Russia]
GCHQ	Government Communications Headquarters [UK]
GPO	General Post Office [UK]
GSMC	Global System for Mobile Communications [UK]
HCSCF	House of Commons Standing Committee F [UK]
HCSCF	House of Commons Standing Committee F [UK]
HCSCTI	House of Commons Select Committee on Trade and Industry [UK]
HCTISC	House of Commons Trade and Industry Select Committee [UK]
HLR	Home Location Register
HM	Her Majesty's [UK]
HMC&E	Her Majesty's Customs & Excise [UK]
HMIC	Her Majesty's Inspectorate of Constabulary
HMSO	Her Majesty's Stationery Office [UK]
IAC	Inter-Application Communication
IBM	International Business Machines
ICC	Interstate Commerce Commission [US]
ICF	Internet Crime Forum [UK]
IEEE	Institute of Electrical and Electronics Engineers [US]
IMAP	Internet Message Access Protocol
IMIS	Institute for the Management of Information Systems [UK]
IOCA	Interception of Communications Act [UK].
IP	Internet Protocol
IRC	Internet Relay Chat
IRS	Internal Revenue Service [US]
ISDN	Integrated Services Digital Network
ISP	Internet service provider
ISPA	Internet Service Provider Association [UK]
IT	information technology
IT&T	International Telephone and Telegraph [US]
IUPF	Internet Users Privacy Forum
KGB	Komitet Gosudarstvennoy Bezopasnosti [Committee for State Security, USSR]
LIAFIC	Library Association for the Freedom of Information Campaign
MI5	Military Intelligence 5 [UK]
MI6	Military Intelligence 6 [UK]
MIA	Military Intelligence Agency [US]
MIT	Massachusetts Institute of Technology [US]
MP	Member of Parliament [UK]
MSC	Mobile Switching Centre
NAACP	National Association for the Advancement of Coloured People [US]
NAMPS	Narrowband Advanced Mobile Phone Service [US]
NCCL	National Council for Civil Liberties [UK]
NCIS	National Criminal Intelligence Service [UK]
NGO	non-governmental organisation
NIJ	National Institute of Justice [US]
NIPC	National Infrastructure Protection Centre [US]
NIST	National Institute of Standards and Technology [US]
NSA	National Security Agency [US]
NSTAC	National Security Telecommunications Advisory Committee [US]

NTAC	National Technical Assistance Centre [UK]
OPASTCO	Organisation for the Promotion and Advancement of Small Telecommunications Companies [US].
PCS	Personal Communications Services
POID	Post Office Investigation Division [UK]
POP3	Post Office Protocol Version 3
POST	Parliamentary Office of Science and Technology [UK]
POTS	Plain Old Telephone System
PR	Public Relations
PTO	Public Telecommunications Operator
RAND	Research and Development [US]
RCA	Record Company of America [US]
REMOBS	Remote Observance
RIF	released in full
RIP	released in part
RIPA	Regulation of Investigatory Powers Act [UK]
RIPB	Regulation of Investigatory Powers Bill [UK]
RNS	released [with] non-substantive [deletions]
RUC	Royal Ulster Constabulary [UK]
SIS	Secret Intelligence Service [UK]
SNP	Scottish Nationalist Party [UK]
SORM	Sistema Operativno-Rozysknykh Meropriyatii (System for Operational-Investigative Activities) [Russia]
STTCPUSHRCC	Subcommittee on Telecommunications, Trade and Consumer Protection of the United States House of Representatives Committee on Commerce
TBI	Tennessee Bureau of Investigation [US]
TIASF	Telecommunications Industry Association Standards Forum [US]
TUC	Trade Unions Council [UK]
TUFF	Telecommunications UK Fraud Forum
UK	United Kingdom
UKERNA	United Kingdom Education and Research Networking Association
UN	United Nations
US	United States [of America]
USAFOSI	US Air Force Office of Special Investigations
USBATF	US Bureau of Alcohol, Tobacco and Firearms
USCCGO	United States Congressional Committee on Governmental Operations
USDEA	US Drug Enforcement Administration
USDoD	US Department of Defence
USDoJ	United States Department of Justice
USEIA	United States Electronics Industry Association
USFDA	US Food and Drug Administration
USHCUAA	United States House Committee on Un-American Activities
USIRS	US Internal Revenue Service
USSR	Union of Soviet Socialist Republics
USSSCSGORIA	United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities
USTA	United States Telecommunications Association
USTIA	United States Telecommunications Industry Association
VLR	Visited Location Register

List of Figures.

List of Diagrams.

List of Tables.

Thesis Abstract.

Informatisation was introduced as a functional parameter in social and political research in 1978 (Nora & Minc 1978). Today, nearly a quarter of a century later, popular and academic political debates in the West appear to be growing increasingly aware of the intense interaction between information technology and social development. This project follows in the footsteps of this increased awareness and explores the meaning of digitisation for the socio-political concept of citizens' privacy.

This project seeks to contribute to a wider body of literature that desires to provide meaningful answers to the following questions: **(1)** what sociotechnical trends are evident today in information privacy policies in the United Kingdom (UK) and the United States (US)? **(2)** What particular political visions do these trends seem to favour and what do these visions appear to suggest for the future of citizens' privacy in the West? **(3)** What is the potential importance of digital networking for practices of social management and control, both by governmental decision centres and commercial bodies?

As case study for the above issues, the eventful appearance of two recent legislative works has been selected: the *Regulation of Investigatory Powers Act* (RIPA), enacted by the UK parliament in July 2000; and the *Communications Assistance for Law Enforcement Act* (CALEA), enacted in the US in 1994. Both Acts, which have yet to be fully implemented, in effect make it mandatory for all telecommunications operators and service providers to, among other things, ensure that their customers' communications can be intercepted by law enforcement and intelligence organisations, whose interception capabilities have been seriously hampered by the digitisation of telecommunications during the past few years.

The project combines quantitative and qualitative data on RIPA and CALEA, which have been acquired through open-source, restricted or leaked government and industry reports on the subject, as well as through a number of interviews with informed individuals representing different sides of the communications interception (CI) debate. The development of communications interception is thus placed into the context of complex relationships between political actors, such as national policy experts and government advisors, state and corporate decision-makers and members of regulatory bodies.

Part I INTRODUCING THE DEBATE

Chapter One

Information Society and Social Control

1.0.0. Communications Systems and Social Development.

The academic preoccupation with communications systems and their role in social development is hardly recent. Nearly half a century ago, the pioneers of what we now consider to be communications science were the first to introduce into the wider sociological debate the proposition that the unrestrained evolution of a dynamic communications system is a crucial precondition for a nation's economic, social and political growth (Shannon 1958; 1959; Lipset 1959; Pool 1959). By 1964, the findings of research conducted by Western scholars on industrialised as well as on developing nations[1], had enabled Wilbur Schramm to declare that

> [w]ithout a sophisticated and efficient development of communication, the base of population, co-operation, industrialisation, education and skills needed in a modern industrial society cannot possibly be established [Schramm 1964:41].

Schramm's assertions were also informed by the innovative work of a number of post-war economists, sociologists and political scientists (Parker 1973:620), in particular by F.W. Frey , K.W. Deutsch, J.J. Spengler and W.W. Rostow, who, in his *Stages of Economic Growth*, explicitly described human societies as "interacting organisms"

[1] Including such classic works as Almond 1960; Cutright 1963; Smythe 1954; Shannon 1958; Pye 1963; and Carter 1959.

(Rostow 1960:2)[2]. For these analysts, structured institutions of communication constituted the essential networking element that synchronised disparate variables of socio-economic development and ensured their smooth amalgamation, thus facilitating the stable character of social organisation (Deutsch 1963:77; Frey 1973:396). It was this amalgamation, enabled by efficient communication, that provided decision-makers at all levels with information essential for rational calculation and planning (Spengler 1963:211).

1.0.1. The Idea of the Information Society.

The concept of the 'information society', coined in 1978 by French scholars Simon Nora and Alain Minc (Nora & Minc 1978), is a direct descendant of Schramm's reasoning. As a social term, informatisation stems from the view that digitisation[3] signifies the emergence of a new paradigm of technological reasoning and is the primary contributor to the reformation of organisational practices in advanced post-industrial societies. Proponents of informatisation maintain that the scale of this reformation is both large and embracing enough to justify the proclamation of a new historical paradigm –that is, a period of major historical change characterised by a new mode of development, which is described as "the informational mode of development" (Castells 1989:12).

The information society model consists of three central elements: the technological, the financial, and the societal (Miles 1988:7-8). The technological element attests to the primarily technical variations between the industrial and information societies and includes both the decreasing cost of information processing (Russell-Neuman 1991:4; Woods 1993:95) and the shrinking size of digital storage and processing equipment (King 1984:3; Heap *et al.* 1995:93; Woods 1993:110). The financial element addresses the economic regeneration by digitisation of consumer capitalism and includes the falling cost of electronic communications (*Economist Magazine* 1995:5[4]; Dordick & Wang 1993:26) and the introduction of new consumer services[5] and investments (Department of Trade and Industry 1996:7; European Commission 1995:13). It also

[2] Rostow's third condition for economic growth is the provision of rapid emergence of a political, social and institutional framework that would actively support and sustain the human impulses for development and give economic growth a continuous character (Rostow 1960:38ff).
[3] The technical features of digitisation are described in section 6.2.0.
[4] According to the Economist, "[t]he death of distance as a determinant of the cost of communications will probably be the single most important economic force shaping society in the first half of the next century" (Economist Magazine 1995:5).
[5] Including the unprecedented development of the so-called 'service sector', which has steadily increased in proportion and size since the late 1960s in Western economies (Gilpin 1975:166; Porat 1978:73ff).

includes the dynamic transformation of production systems facilitated by advanced digital techniques (Miles 1988:9; Dordick & Wang 1993:124). The latter render corporate structures "information-dependent" (Cruise-O'Brien & Helleiner 1983:3) –a phenomenon through which information processing becomes

> the core, fundamental activity conditioning the effectiveness and productivity of all processes of production, distribution, consumption and management [Castells 1989:18].

Thus, digital information mechanisms operating in an information society are viewed as primary determinants of economic growth, as well as core elements of the predominant mode of production, to the extent that one cannot adequately address economic development without reference to informatisation.

Finally, the societal element in information society theories attests to the quantitative and qualitative change of the channels of information through which social exchange takes place and assumes meaning. In other words, as increasing segments of social activities are mediated by electronic communications (Poster 1990:1), the digital infrastructure of the information age gradually becomes proportional to the entire spectrum of human activities and desires (M. Dertouzos[6] in European Commission 1995:20). In essence, digital information systems do not represent a new form of social discourse imposed upon an older one, but rather a complex weaving of different means of expression within that same discourse.

The above features outline a vision for change, but also a developing reality that is already incorporated with, and incorporates, a variety of technological, economic and social experiences in the West.

1.1.0. Two Competing Visions of Informatisation.

Nevertheless, the phenomenon of informatisation does not occur in an ideological vacuum. As digital communications systems interact with the social, political and cultural environments in which they are produced and used, they contribute to the rise of new social expectations, cultural ethics and moral attitudes. Inter-connectivity, globalisation, competitiveness and deregulation are some of the keywords used to

[6] The late M. Dertouzos was Head of the Massachusetts Institute of Technology's (MIT) Media Laboratory.

embody these new social and political parameters[7]. Technological change does not necessarily give shape to these parameters. As demonstrated in following quote from one of the corporate architects of the information society, technological development is simply one of the means by which specific political visions have been carried through to the new millennium:

> [a] fast, world-wide deregulation of information is needed [...] to create the conditions enabling us to take advantage of the information society. Part of what we have to do is to reduce monopolies. Monopolies are not compatible with an information society, which is dominated by free-market flow, a free flow of ideas and no borders [C. De Benedetti[8] in European Commission 1995:15].

Indeed, the ideological links between economic liberalisation and social informatisation have traditionally been particularly strong and were instrumental in the Reagan and Thatcher administrations' decision to deregulate telecommunications –a move which completely changed the landscape of the UK and US sectors during the 1980s and early 1990s (Hills 1986:24ff; Jonquieres 1989). According to this vision, the information society project belongs to the private sector and, as such, is incompatible –as De Benedetti suggests in the above quote– with substantial governmental intervention. Informatisation, therefore, is seen as the vehicle by which civil society liberates itself from governmental conditioning and supervision and discovers consumer inter-dependence within self-regulated global markets (King 1984), as well as within non-statist models of political negotiation, such as direct participatory democracy (Masuda 1981:33ff; Abramson *et al.* 1988; Barber 1984; 1988; Hollander 1985; Slack 1987) based on secure electronic networking (Rheingold 1993).

But there is also another view of the information society which sees informatisation as a force broadening the interface between civil society and government, thus increasing the ability of organised state bureaucracies to exercise electronic forms of surveillance and social control over the networked populace (Williams 1974; Fisk 1994; Manwring-White 1983; Ackroyd *et al.* 1980; Donner 1988; Zuboff 1988). This view interprets the emergence of digital technologies as being virtually synonymous with increasing governmental constraints over the political liberties of citizens:

[7] On this see Dale 1996:28ff and Giddens 1991:27. Commenting on the Japanese experience, Dale puts forward the idea of a particular climate, or atmosphere, characterising the information society, one that "conflat[es] the social self with the universal order, leav[ing] no margin for expressing [one's] private ideas that may be dissonant with the social order itself" (Dale 1996:41).

[8] C. De Benedetti is chairman and chief executive of Olivetti, SpA.

> [t]here is an uncomfortable aura of *1984* in all this. Thus it is not difficult to visualise how the computer utility might be perverted until it degenerated into nothing more than an instrument of total political control –the omnipresent eyes and ears of "big brother" [Parkhill 1979:89].

The "uncomfortable aura of *1984*", to which Parkhill refers, stems from his belief that, ultimately, digitisation will reinforce rather than hamper the centralised surveillance capabilities of contemporary Western nation states.

1.1.1. Social Control and Surveillance.

In essence, both views outlined above are concerned with the impact of digitisation on the degree of social control facilitated by communications technologies in contemporary Western societies. The term 'social control' is used here in the traditional Durkheimian sense of the striving by organised societies to achieve a degree of social regulation consistent with certain moral and legal principles[9]. The nature of social control can, but does not have to, be coercive. In parliamentary democratic regimes social control includes the legal and administrative instruments through which social disobedience is deterred, hindered or even punished once it has occurred. These instruments can assume various forms and, in their loosest sense, can include conditioning through education or the appropriation of social benefits to reward obedient social parties (Ripley 1966:ix, xi). In their more concrete sense, however, they include military, law enforcement and intelligence apparatuses, as well as a host of management techniques designed to assure stability and cohesion in large-scale national structures (Rule 1973:20). Undoubtedly, the political mandate of the use of these techniques is to preserve the authority of representative and appointed governing institutions, as well as to deter threats against their integrity, their autonomy and, ultimately, their ability to exercise power (Gill 1994:55; Spitzer 1985:325).

State-sponsored communications surveillance, that is, the ability of state authorities to access and comprehend the pattern as well as the content of communications messages exchanged within and beyond their national territory, is an integral part of the policing techniques of social control in modern nation states. Traditionally, the principal method of policing communications networks has been CI. The term describes the act of

[9] This is the issue of the 'social order', considered most explicitly by Durkheim and his functionalist inheritors; see Cohen & Scull 1985:5.

intercepting telecommunications messages, usually through a main switch post in the telecommunications network (Carr 1998§1.3)[10]. It is not to be confused with 'bugging', which suggests audio surveillance through concealed microphones not linked to the telephone network[11]. The legal sanctity of CI derives from the age-old practices of state-sponsored mail and oral interception. Specifically, CI signifies the transference of the principles of mail and oral interception into the domain of electric and electronic communication.

The phenomenon of state-sponsored CI is crucial for the two competing visions of the information society, outlined above. Specifically, the impact of digitisation on the practice of CI is seen as indicative of the degree of intrusiveness that practices of social control will assume in the information society. Consequently, the future course of a host of fundamental principles of Western ideology, such as personal liberty, freedom of expression and even personal privacy, is seen to be dependent on the unfolding effects of digitisation upon the telecommunications infrastructure (Wilson 1988:80ff).

1.2.0. Digitisation and CI: RIPA and CALEA.

There is no empirical confirmation of this tendency to associate technical developments in the field of telecommunications with the future nature of state-sponsored surveillance. What is more, this association is often characterised by deterministic overtones, which underestimate the significance of the economic, as well as the socio-political and legislative environments in which technologies are conceived, developed, implemented and used.

Broadly speaking, however, technological trends have shaped some academic views on the future of social control: the technical features of digital networking have contributed to the widespread belief that decentralised communications networks, including the Internet, are somehow uncontrollable. Observers have discussed the Internet as a self-regulated social structure, whose technical properties virtually exclude the possibility of governmental censorship or other forms of structured regulation (Depla & Tops 1995).

[10] Detailed technical analysis of CI is provided in Chapter six.

[11] Both wiretapping and bugging are specific terms related to 'eavesdropping' –a general designation which describes any attempt of third person to overhear conversations without the knowledge or consent of one or more of the participants.

Indeed, during the early 1990s it emerged that there was considerable basis to back such claims. In the US, and later in the UK, governmental law enforcement and intelligence agencies disclosed that the technical specifications of telecommunications digitisation were overpowering traditional models of CI. It was claimed that the binary transformation of oral messages, the packetisation of digital data, as well as the introduction of digital switches and digitally-enhanced wireline and wireless user services, threatened state-sponsored CI with virtual extinction (Yarbrough 1999:4-5; Boucher & Edwards 1994; Morris 1998).

Government agencies in the US and the UK acted swiftly to contain these threats to their interception capabilities. Two unprecedented pieces of legislation emerged, through which the US and UK governments demanded that the telecommunications industry modify the technical features of digital networks so as to make them intercept-friendly for a host of state law enforcement and intelligence organisations. In the US, the Bill version of CALEA was approved by Congress and enacted by the president in October 1994, while in the UK RIPA became law a few years later, in July 2000. Both CALEA and RIPA signified the first instance in the history of US and UK telecommunications where virtually all communications service providers (CSPs) were required to modify the technology of their systems in accordance with law enforcement requirements (Berman & Dempsey 1996) –"the first time in our history", as the American Civil Liberties Union (ACLU) put it, "that an entire industry [has been] required to alter its technology so the government would be guaranteed success in its snooping" (Steinhardt 1995).

It is difficult to underestimate the significance of these developments: in the UK, the National Crime Intelligence Service (NCIS) has warned that, in the absence of RIPA, the UK government's CI capability will "move to redundancy" (HCTISC 1999a). Additionally, in the US, the Federal Bureau of Investigation (FBI) has described the issue of facilitating digital CI as "one of the most difficult [and] complex [...] ever to confront law enforcement" (Freeh 1997b).

What is more, consensus between government and industry bodies over the scope and scale of CALEA and RIPA schemes has proven particularly elusive. The sheer financial scale of the required implementations –which include the modification of millions of digital switches throughout the two nations– has alarmed industry representatives, while

US and UK civil liberties watchdogs have warned of the legal ramifications of building interception capabilities into telecommunications networks. Consequently, in the US, numerous court cases involving the FBI, Department of Justice (DoJ), as well various telecommunications industry associations and civil liberties groups have marred the CALEA debate and are still unfolding as this thesis is heading for submission. As a result, almost eight years following CALEA's enactment, the legislation has yet to be fully implemented.

A similar situation appears to be developing in the UK, where the vagueness that characterises RIPA's mandates has caused widespread scepticism among the industry and civil liberties advocates over the legislation's ability to withstand a series of legal challenges that will undoubtedly be directed against it (Sutter 2001)[12]. The technical standards of the legislation have yet to emerge, almost 18 months following RIPA's enactment –probably an indication of the long road that lies ahead until the legislation's requirements are fully agreed upon and implemented.

1.2.1. Two Transatlantic Case Studies.

It follows from the above that both CALEA and –especially– RIPA are still subject to heavy construction. Yet their emergence is of overwhelming significance for research, inasmuch as they represent the first attempts by US[13] and UK governments to define the legal, technical and administrative parameters of CI in the digital environment. Their future will therefore be highly instrumental in outlining new models of state sponsored surveillance and, consequently, social control in the context of the information society.

In an important sense, the unfinished state of CALEA and RIPA is due to the complexity of the CI debate. By simply reading the text of the two Acts one forms the impression of them as absolute commands delivered by security-oriented policy makers to the telecommunications industry. Yet the reality is much more convoluted. CALEA and RIPA represent attempts to strike a balance between policing and national security, on the one side, and individual liberties and open consumer-oriented markets on the other. What is more, the CI debate is conducted within the context of increasing market deregulation at he local, national and international levels, which often tends to marginalise state objectives –including national security objectives– in favour of

[12] On the legal challenges to RIPA and CALEA see section 8.2.0
[13] In the case of the US, the first attempt by any government in the world.

corporate and consumer goals. It is within this very context that the concept of CI is discussed in the present thesis, in an attempt to examine CI in the information society while avoiding the deterministic temptation to ignore elements of the debate that do not appear to match a set of monolithic, prescribed criteria.

1.3.0. The Structure of the Thesis.

The considerable absence of an adequate body of political and sociological research literature on CI is indicated in chapter two, *Review of the Literature*. This absence has primarily shaped the methodological framework of this study –which is outlined in chapter three, *Some Considerations of Method*– and has steered it toward the adoption of a threefold structure.

Initially, there is offered an account of the historical context of telecommunications regulation in the UK and the US. This is provided in chapter four, *The Government and Telecommunications in Historical Context*, which describes the role of concepts of national security and policing in shaping the legislative and political parameters of telecommunications regulation. Following, in chapter five, is a detailed account of the uses of CI practices by UK and US state agencies since the emergence of telephony and until the end of the Cold War. This chapter is entitled *The Interception of Communications in Historical Context*.

In Part III, an account of recent developments in CI in the digital environment is presented. The different technical specifications between analogue and digital CI are outlined in chapter six, *The Techniques of Interception*, with reference to the specific technical dilemmas that permeate the digital CI debate. In chapter seven, *Elements in the Digital Interception Debate*, the role of CALEA and RIPA in the wider CI debate is outlined, with reference to the particular findings of research conducted in the context of the present thesis.

In the final part, Part IV, there is offered an evaluation of the research findings. This is accomplished by discussing the findings themselves, as well as in the context of the existing research literature. While chapter eight, *Future Trajectories of Interception*, will attempt to place this research in the context of available literature and data, the last chapter, *Digital Communications Interception and Social Control*, will suggest a number of concluding observations, accompanied by suggestions for further research in the field of CI and surveillance in general.

Chapter Two
Review of the Literature

2.0.0. Introduction

It is difficult to understate the role of the uses of CI and related technologies in the overall history, as well as in the everyday affairs, of modern nation states. As Spindel (1968) graphically puts it,

> [n]ations have been born and governments overthrown, thousands of lives lost and others saved, by the use of techniques and devices virtually unknown to the general public [Spindel 1968:7].

Indeed, the clandestine nature of the practice of CI has effectively prevented the widespread dissemination of its political significance within the public arena. Nevertheless, American and British researchers often recognise that the sophistication and aggressive use of such clandestine techniques have assisted their countries' governments in achieving integral political, diplomatic and military objectives which would have been unrealisable through conventional bureaucratic means (Godson 1996:8-9, 254; Kahn 1967).

2.0.1. The Crucial Dichotomy in Political Research on CI.

Researchers seem to be eager to explore the uses and significance of CI techniques in international affairs. As a result, a series of works with both empirical and analytical value have been presented over the years (Mahl 1998; West 1983b; Breckinridge 1986;

Campbell 1999). This eagerness is even more discernible within specific segments of the research literature in which the practices of CI are examined in the context of former or existing Stalinist regimes around the world (Minnick 1995; RAND 1992; Baleanu 1995). Rather expectedly, the experience of the USSR is a prominent theme (Ball 1989a, 1989b; Richelson 1986; Knight 1990; Romerstein & Levchenko 1989) [1]. Equally large parts of the literature discuss in considerable detail the Cold War uses of CI made by Western intelligence services against Stalinist regimes (Andrew & Gordievsky 1990; Milano 1995; Murphy *et al.* 1997)[2].

The extent to which painstaking research has been conducted into the practice of CI in international affairs by Western intelligence services is indeed surprising, especially considering the politically sensitive nature of the issue under scrutiny. Technical revelations on CI are no exception (Melton 1993): recently, a study on the subject, commissioned by the European Union, reported that

> [m]iniaturised inductive taps recorders have [...] been used [by the National Security Agency (NSA)] to intercept underground cables. NSA and other Comint[3] agencies have spent a great deal of money on research into tapping optical fibres, reportedly with little success. But long distance optical fibre cables are not invulnerable. The key means of access is by tampering with optoelectronic 'repeaters', which boost signal levels over long distances. It follows that any submarine cable system using submerged optoelectronic repeaters cannot be considered secure from interception and communications intelligence activity [Campbell 1999:43].

The appearance in the public arena of such detailed technical information –often unapproved by governments[4]– on CI is a relatively recent phenomenon, which reflects an increasing degree of official and unofficial interaction between researchers and intelligence sources, as well as, perhaps, increasing eagerness by researchers to concern themselves with the subject.

However, research literature on CI does not reveal similar degrees of eagerness in exploring domestic uses of CI by law enforcement and other government agencies

---

[1] In addition to the interest of researchers and readers alike, the post-Cold War explosion of research into Soviet CI techniques has been furthered by the tidal waves of release of previously classified documents by Western intelligence agencies. This applies especially to the US (see for instance Verton 2000a; Kramer 2000; CIA 1953, 1958, 1962a, 1962b).

[2] Interestingly enough, a considerable number of these texts resulted from the co-operation between American or British and Russian intelligence researchers or former officers, often with access to declassified segments of US, UK and Russian state archives.

[3] Comint: communications intelligence.

operating within Western parliamentary-democratic structures. In this sense, British and American research literatures on CI reveal a crucial dichotomy, a conspicuous double standard: on the one hand, the technical, social and political meanings of CI techniques applied by, or against, adversary nations and groups have been attended to by scholarly works produced *en masse*; on the other hand, the same techniques have been widely absent from academic discourse when applied by Western governmental agencies to the internal policing of their own citizen base. Most of the few researchers who have seriously concerned themselves with the subject, have been legal scholars[5]. The principal social science disciplines, namely sociology and political science, have remained largely silent. The reasons are quite possibly related to the political controversy that surrounds the issue and quite certainly to the secrecy and, consequently, lack of information on the subject.

2.1.0. UK: The MI5 and Related Mysteries.

Nowhere is this absence of domestic CI manifested more vividly than in the segment of the research literature which concerns the British experience. Specifically, of the only two[6] books in existence solely devoted to international CI, none is a product of academic research. The earlier of the two (Wingfield 1984) was produced by a surveillance professional operating in the private sector and is presented as a practical manual on the field of CI. In the book's lengthy introduction, completely based on unclassified sources of information, one can detect an uneasy mysticism generated by the considerable lack of basic data on CI –a sense that is all too familiar in numerous such texts:

> [a]ccording to Home Office guidelines, no private telephone member may be tapped without the approval of the Home Secretary [.... Yet these regulations] do not apply to MI [(Military Intelligence)] 5 [...], who apparently have *carte blanche* to spy on whomever they choose, whenever they choose, with no need to justify their actions to anybody at all [.... I]n Britain, nobody really knows how widespread the surveillance activities of government agencies are [ibid.:28, 31].

The remaining book on the British experience (Fitzgerald & Leopold 1987) is the product of the investigative research conducted by two journalists. Its pages are marked

---

[4] For an introduction to the phenomenon of US classified information leaks to researchers and to the press see Verton 2000b; Simpson 2000.

[5] See, for instance, Lapidus 1974; Murphy 1965; Westin 1962; Leigh & Lustgarten 1989. Most of these texts concern the legal aspects of CI and engage in little, if any, social or political discussion of the practice. The exception to this is Akdeniz *et al.* 2001; Taylor & Walker 1996; as well as Dash *et al.* 1959, of which more later.

by heavily polemical rhetoric, which is characteristic of many works on CI. The book is, in effect, a unified attempt to address two main issues: firstly, to raise suspicion concerning official government data on CI (ibid.:14ff); secondly, to argue that the lack of popular supervision over the CI activities of state intelligence services could become the vital parameter leading to the creation of an Orwellian state structure in late 20th century Britain –a development that, according to the writers, ominously hangs in the balance:

> Britain in the eighties is not a police state in the classic, Orwellian sense. What has prevented this, however, are not the laws and administrative regulations governing tapping which pass as 'accountability' in the case of the intelligence services. Rather, our current defences against total surveillance lie in the institutional and financial constraints put on the spies and, above all, on the restraining influence of [legal] precedent [ibid.:35].

In their effort to illustrate their case, the two co-writers present us with yet another characteristic of many works on the subject of CI[7] and surveillance in general. Namely they present an impressive body of analytical legal and historical research (ibid:64ff) existing side by side with reductionistic interpretative idiosyncrasies. The latter unmistakably reflect the pugnacious social context of Thatcherism's politically polarised Britain: on one side of the fence stand the unified 'reactionary' forces of the Conservative Home Office administration, the General Communications Headquarters (GCHQ), the MI5, the Royal Ulster Constabulary (RUC), the Post Office Investigation Division (POID) and British Telecom (BT), while on the other side are Labour Party militants, miner activists, trade unionists, the Campaign for Nuclear Disarmament (CND), the Communist Party (CP), Plaid Cymru and Irish Republicans (ibid.:24, 58-9, 82).

Yet there is an important sense in which this polarisation in the political interpretations of CI and related techniques has been maintained in the British bibliography regardless of the politics of the particular government in charge. An illuminating case in point is one of Tony Bunyan's (1976) earlier works on British intelligence institutions, entitled *History and Practice of the Political Police in Britain*. In the section of the book devoted to international CI (ibid.:196ff), one can detect an ideological framework according to which the practice of CI is virtually synonymous with the unjustified invasion of privacy. Harold Wilson's Labour government is seen as having little, if any, effect on

---

[6] This number does not include the collection of essays found in Campbell 1981, as most essays in this volume concern international uses of CI by the British and other governments.
[7] Including the work of Ackroyd *et al.* 1980.

that synonymity, whose institutionally-embedded endurance has the ability to survive the superficial ideological features of temporary party-affiliated administrations[8]. Ultimately, it is once again the very institutional intimacy[9] between the government, the Criminal Investigation Department (CID), Special Branch, Her Majesty's Post Office and BT, which facilitates some of the more Orwellian uses of CI (ibid.:202), as well as the disablement of popular oversight. Each time allegations of unlawful CI practices emerge in public,

> [t]he pattern is clear. The local police deny it, the Post Office find other explanations for the occurrence, and the government will neither confirm nor deny the charge [ibid.:209].

On the directly opposite side of the debate one may find rare instances[10] in which law enforcement or Home Office officials have endeavoured to publicly justify the practice of CI. C.H. Rolph's[11] (1973) paper entitled *The British Analogy* is largely representative of such endeavours, which are, on the whole, largely descriptive rather than interpretative. Thus, they are characterised by the lack of any political considerations of, or critical attitude over, the practice and culture of CI[12]. What is often proposed instead is the consideration of CI as a vital institutional practice of government, whose essence and political significance is not in any fundamental way different to that of, say, tax revenue assessment or traffic policing:

---

[8] Bunyan (1976) wastes little time in asserting that "[t]he government [...] does not control the state; rather, the institutions making up the state –of which the government is one– act together in commanding state power" (ibid.:2). Evidently, Bunyan's approach contains elements of the belief – widespread among the British left –that Wilson's Labour government never managed to assume administrative control over the CI activities of the British intelligence establishment. Indeed, Wilson's eventual resignation prompted rumours of sinister explanations, including allegations by MI5's Peter Wright, of a plot by intelligence officers to destabilise him because of his government's alleged links with the Soviet Union (Wright 1987:363-365; see also Leigh 1988; Ramsay 1996; Norton-Taylor 1997).

[9] "The role of these institutions and the repressive state agencies in liberal democracies is to ensure the reproduction of the capitalist system [.... I]t is possible to see the interdependent nature and totality of the practices of these state agencies in relation to the dominant interests in society as a whole, namely those of capitalism" (Bunyan 1976:3, 289).

[10] Arguably, the rarity of such instances is because law enforcement and intelligence organisations see little use in publicly defending a largely clandestine practice which has traditionally enjoyed almost complete governmental protection and which has never been denounced by a considerable segment of the citizen body or its elected representatives. Additionally, the aforementioned rarity reflects the absence of a sufficient body of official interpretations of CI on behalf of the British state. This tendency has not gone unnoticed by British scholars; Gill (1994), for instance, notes that "the limited nature of the British reports reflects the lack of any serious competitor to the centralised power of the executive branch" (ibid.:31).

[11] A former police officer.

[12] A recent example of this tendency can be seen in Curry 1999. Older examples include official documents published by the British government over the years, such as Command 7873 1980; Command 9843 1985 and Command 108 1987.

> In 1957 [...a C]ommittee [of Privy Councillors[13]] found that [communications] interception had no basis in law, whether common law, acts of Parliament or what is called royal prerogative: the only basis the Committee could discover was *long usage*. This is another way of saying that it is unlawful but no one cares to stop it. And *long usage*, though not so long as you might suppose, is the basis of a very high proportion of the powers exercised by the police. As a matter of interest, the police in England were regulating road traffic for very many years before they were given the legal power to do it by the Motor Car Act of 1903 [ibid.:395, his emphasis].

Of the strictly academic approaches to CI, there can be found no more than three works offering other than an incidental (albeit brief) approach to the subject. These are the works of Lambert (1986), Gill (1994) and Lustgarten & Leigh (1994). The first contains a brief section on the uses of CI by law enforcement in which a crucial dichotomy is established –one that permeates the scant literature on surveillance techniques. The dichotomy occurs between HM Police Constabulary, which makes limited use of equally limited CI resources, and the security services, which are believed to enjoy unlimited use of CI means (Lambert 1986:207-8)[14]. The lack of basic official information on CI facilitates a detectable overlapping between academic and popular works on the subject. In both genres the absence of accountability over CI practices is presented in unfavourable terms:

> [i]t is not surprising in the light of the fact that the use of electronic surveillance is barely acknowledged by the authorities, that there is no legislative basis for it. It is a secret activity over which there is no formal control [ibid.:208].

There also appears to be an overall suspicion as to the credibility of officially approved figures on the extent of CI use, the latter being described as having remained at "surprisingly stable" (ibid.:212) levels over the years. Gill (1994), takes advantage of this statistical stability and uses it to engage in what has become a frequent occurrence in academic debates on CI, namely a great deal of inference, leading to scepticism about the plausibility of governmental data:

> [o]fficial figures on the extent of tapping have remained constant for 20 years with Home Secretaries issuing between 350 and 470 warrants a year since 1969 while the number of telephone lines has increased from 8 million to over 20 million [ibid.:168].

[13] Rolph (1973) is referring here to Command 283 1957.

[14] This belief has been largely formulated by reference to the wording of official reports, such as Command 108 1987:§53-4.

Inference, however, leads also to a crucial shift in the point of interest of the researcher. Revelation of the true extent of the practice of CI by state institutions is rendered irrelevant, as 'truth' becomes an ideal bound by the red tape of bureaucratic protocol. This phenomenon is said to occur to such an extent that it appears to elude even bureaucrats themselves:

> [a]s this compounded distortion proceeds upwards through several levels of the [intelligence] organisation, the possibilities of superiors knowing what is actually going on becomes very slight [Peters 1984:136, ctd. in Gill 1994:50].

Instead, the researcher draws his or her attention to the question of whether 'truth' should be allowed to elude from intelligence administrators and citizens alike in the context of parliamentary democracy. Indeed, what is it about certain segments of law enforcement and intelligence apparatuses that has allowed them to evolve –and, to a large extent, remain– in the shadows of Western democratic transparency? Gill's (1994) reply concords with those of numerous other scholars[15], who claim that it is the administrative centrality and political indispensability of these institutions that has permitted them to evolve in relative isolation from parliamentary and popular oversight:

> [t]he basic mandate of all security intelligence agencies is to defend the parent state against threats to its integrity and autonomy, in other words, its ability to exercise power [ibid.:55].

Eventually, it is the dramatic absence of official information on CI and related practices that urges Gill (1994) to openly question the political wisdom behind the operative isolation of intelligence institutions from democratic principles:

> there is inadequate democratic control of state structures in the UK, particularly of the security intelligence agencies and [...] this poses such a threat to democratic forms that it requires fundamental change [ibid.:39].

This democratic deficiency that allegedly resides at the very core of the political meaning of CI techniques, is a recurring theme that characterises another relatively recent study by two legal scholars, Lustgarten & Leigh (1994). Though not directly concerned with CI, their detailed comparative approach deconstructs the legal, political and essentially cultural context in which CI is authorised and practiced. In a manner similar to Gill (1994), the authors question the practical plausibility of executive control

[15] Including Ackroyd *et al.* 1992:27; Baxter 1990:1; and Turk 1982, who asserts that "political [i.e. intelligence] policing may be understood as the sharpest cutting edge of the multidimensional effort to

over security and intelligence operations within the Western parliamentary democratic state. Perhaps predictably, the two scholars find that intelligence and security are concepts that are not alien to the roots of parliamentary-democratic concepts of governance, though the lack of structured monitoring procedures over these practices can threaten the rigidity and flexibility of those very roots (Lustgarten & Leigh 1994:217). Essentially, it is the very axiomatic placement of intelligence institutions within the contemporary democratic state that allows them relative freedom from principles of transparency. Thus when national security is perceived to be at stake, it is usually the rules of democratic accountability that are modified to accommodate intelligence quotas, as opposed to the contrary (ibid:24).

2.1.1. US: McCarthyism, Big Government and Watergate.

There are arguably four broad factors that have facilitated greater activity in popular and academic discourses on domestic CI in the US, compared to the UK: one, the more lax adherence to secrecy by the US Federal and local government[16], as opposed to the UK's Executive Branch[17]; two, the distrust –traditionally widespread throughout the American political culture– of an expansive, interfering government (Wills 1999; PRCPP 1998); three, the experience of, and reaction to, McCarthyism (Schrecker 1986); and four, the wiretapping revelations of the Nixon administration, which began to surface in 1972 and eventually stigmatised the political culture of the nation, in the form of the Watergate affair.

It was the reaction to McCarthyism that sparked what still, 42 years later, remains the most extensive and detailed investigation on international CI ever conducted anywhere in the US or the UK. It was soon after Joseph McCarthy's Senatorial downfall when three academic and legal professionals, Samuel Dash, Richard F. Schwartz and Robert E. Knowlton, were sponsored by the Pennsylvania Bar Association to conduct a coast-to-coast investigation detailing the use and –as the report eventually revealed– abuse of CI methods by law enforcement throughout the first half of the 20th century. The report,

---

accomplish political dominance" (ibid.:160). For a somewhat opposing argument see Bar-Joseph 1995:10, 123.

[16] As highlighted by, among other legal assurances, the Freedom of Information Act (5 USC 552) 1966.

[17] The comparison has been drawn by many authors, including LIAFIC 1980; Rogers 1997; and Wilson 1984, who repeatedly uses the US and Australian Freedom of Information Acts as arguments in favour of the introduction of similar legislation in the UK.

later published as a book entitled *The Eavesdroppers* (Dash, *et al.* 1959) [18], involved the analysis of thousands of eponymous and anonymous questionnaires, as well as hundreds of interviews with police officers, former FBI technicians, telephone company officials and workers, District Attorneys and wiretapping equipment manufacturers in dozens of US states.

Meticulously constructed in its 500 pages are three notions that have characteristically marked the US literature on international CI ever since: first, there is the belief that citizens' privacy was a parameter of the telephone network that had been legally ignored and politically suppressed from the very genesis of the telephone system in the US – especially in the larger cities[19]; second, there appears a consistent perception of officially approved government statistics on the domestic use of CI as fundamentally detached from truth in a reckless and perhaps even mischievous manner. A particularly impressive example is that of the state of New York. The writers quote New York Supreme Court Justice W.O. Douglas (1954) who, following his 1953 retirement, claimed that, in 1952, there had been issued by New York City District Court at least 58,000 CI court orders (Douglas 1954:355). According to Dash *et al.* (1959),

> [i]n 1952, the year Mr. Justice Douglas credited with 58,000 wiretaps in New York city alone, the total of wiretap orders acknowledged by New York prosecutors in the entire state was 419 [ibid.:42][20];

third, there is highlighted an institutional interface –elaborate in its complexity, yet straight forward in its operational significance– between law enforcement and the AT&T monopoly, which is viewed as the primary facilitator of unconstitutional CI practices[21]. Specifically, the technical knowledge possessed by telephone company staff is described

---

[18] It should be noted here that –rather intelligently, when considering the political context of the era in which the report was produced– Senator Joseph McCarthy's name, McCarthyism, or even the name of FBI despot J. Edgar Hoover are not mentioned even once throughout the book. Nevertheless, the report is in effect a detailed study against unconstitutional telecommunications privacy invasion by law enforcement in the US, one of McCarthyism's particular trademarks. In addition, Professor Samuel Dash, the report's principal contributor, had been the principal founder and president of the Harvard Voluntary Defenders (est. 1949) and the National Association of Defence Lawyers (est. 1958), organisations that were actively involved both in denouncing McCarthyist tendencies in US legal institutions and in the legal defence of individuals and organisations targeted by the United States House Committee on Un-American Activities (USHCUAA).

[19] "From 1892 until 1938, during which time the police wiretapped regularly in the face of what appeared to be an outright prohibition by the New York legislature, there seemed to be little public concern over this practice and an absence of hostility on the part of the legislature and the courts" (Dash *et al.* 1959:35).

[20] According to Douglas (1954), the apparent discrepancy in the numbers is due to the vast number of CI orders issued on national security grounds and are thus immune to public disclosure (ibid.:101). The latter type of authorisation covered the investigation of so-called 'un-American' activities.

as indispensable for the day-to-day operation of law enforcement CI operations. What is also indicated is the lack of any considerable hesitation on behalf of AT&T local branches to assist law enforcement's CI needs. This is alleged to occur even in the absence of a court order (ibid.:66ff) and often to such an extent as to involve the transference of considerable amounts of workload from law enforcement to telephone company personnel:

> [t]he police of New Orleans do not possess much wiretapping equipment, nor do they need it. Any telephone they wish to place under surveillance can be put on either one of two major telephone company test boards and monitored at the test board station by telephone company employees. Even a tape recording of the conversation will be supplied to the police officer by the monitoring employee [ibid.:123].

Yet the book stops short of unleashing an all-out assault against the institutional facilitators of CI use and abuse by state agencies. The reactionary political meaning of CI practices in post-war US is revealed only in the form of carefully camouflaged hints lurking between the lines of the text reflecting, perhaps, the somewhat confined academic environment that often stigmatised controversial research in the US during the era of the Cold War.

Dash, Schwartz and Knowlton's (1959) conclusions have been repeatedly echoed throughout the scant bibliography on international CI in the US, a significant part of which has been produced by private CI technical experts[22]. The latter divulged their knowledge and expertise in the form of personal accounts and guide manuals aimed toward non-specialised readership. The informational value of such publications consists in the fact that most of these professionals repeatedly shared their expertise with law enforcement organisations that were technically inarticulate in CI methods[23]. One informative such work is by LeMond & Fry (1975) in which, among other things, it is stated that

> if a local law-enforcement official wishes to initiate a wiretap with the proper court approval, dealing with the telephone company is easier than getting a dial tone. Most of the telephone companies around the country will even supply the necessary equipment to the grateful police [ibid.:23].

---

[21] "Much of the ease with which police officers engage in illegal wiretapping depends on telephone company contacts" (Dash *et al.* 1959:72).

[22] It is worth noting here that CI should not be considered a black-boxed technology. There are numerous technical manuals in existence that engage in the micro-mechanics of CI, aimed at a variety of non-specialised or specialised readerships and often displaying a remarkable level of technical precision and detail; see for instance Tsailovich 1999; Larsen 1997; Pollock 1973.

[23] Such instances are anything but rare. There has been a long tradition in the US of law enforcement institutions hiring private investigators to carry out their surveillance operations (Donner 1980:31).

Such dealings between law enforcement and telecommunications carriers[24] are viewed through the –often unsubstantiated– prism of a government administration more aligned with its own intra-institutional agenda, rather than with the privacy interests of citizens. Inevitably, the administration's alleged interests are seen as corrupting regulatory legislation through deliberate discrepancies that leave unwarranted CI practices unaffected[25]: in criticising the Federal Communications Act of 1934[26], LeMond & Fry (1975) assert that it was deliberately designed to prohibit, not the unwarranted practice of CI, but rather the divulgence of any information gathered through such practices in court (ibid.:13)[27]. The Act is indeed considered to be a clear instruction to US law enforcement that "while [unwarranted] wiretapping [is] fine, don't ever let anyone know that you've done it" (ibid.:7).

Finally two individuals are repeatedly mentioned in the text, who, through their actions, shaped the CI debate in the US: former FBI strongman J. Edgar Hoover and former US president Richard M. Nixon. The former symbolises the Bureau's institutional secession –in many ways unprecedented– from the realm of governmental oversight during Hoover's prolonged reign. Accordingly, the extent of CI abuse by the Bureau during that period is seen as an undisclosed segment of modern US history, which may never be fully revealed (ibid.:22)[28]. The latter of the two, Richard M. Nixon, symbolises what could be described as the worst nightmare of both CI advocates and opponents alike: the abuse by a US president of the national security[29] clause to justify the systematic practice of CI in order to achieve political gains for his administration. Nixon's assurances to the public on the governmental use of CI during his administration are cited with heavily ironic undertones, in light of the Watergate[30] affair:

> [n]ow, in the two years that we have been in office, now get this number, the total number of taps for national security purposes by the FBI (and I know because I look not at the information but at the decisions that are made) the total number of taps is less, has been less, than fifty a year [R.M. Nixon ctd in LeMond & Fry 1975:22].

[24] On this issue see also two other works produced in the US by professional CI practitioners in the 1960s, Spindel 1968:106, 112-113 and Carroll 1969:163-4.
[25] See also Spindel 1968:9, 11, 202.
[26] Outdated since 1968.
[27] The reference here is to Section 605 of the aforementioned Act.
[28] One of the most detailed analyses of the way in which J. Edgar Hoover's personal politics shaped the FBI's CI practices during his reign can be found in Theoharis & Cox 1988.
[29] National security is understood here as the ability of a nation's armed forces, as well as intelligence and diplomatic agencies to prepare for and to conduct warfare.
[30] Interestingly, Samuel Dash, the primary contributor in the aforementioned Dash *et al.* 1959 served as chief counsel and staff director of the US Senate Select Committee on Presidential Campaign Activities (a.k.a. the Senate Watergate Committee) from February 1973 to September 1974.

Most works produced in the US by private CI professionals tend to overlap in the information they provide, as well as in their interpretations of it, with the exception of one crucial contribution, namely that of Spindel (1968)[31]. The latter indicates what he perceives as "the tremendous lack of understanding of the technical aspects of electronics" (ibid.:29) on the part of CI legislators and court Justices; he goes on to elaborate:

> [an ...] interpretation by a Federal court declared that if the interception allowed the eavesdropper to overhear a conversation *before* the person for whom the communication was intended heard it, a wiretap was thereby established. On the other hand, if the eavesdropper heard the conversation even a fraction of a second *after* the intended recipient, there was no wiretap. Such technical splitting is difficult to accept in view of the fact that electronic sound travels at the speed of light – 186,000 miles per second. It becomes obvious that it is most unwise to delegate the task of making such decisions or laws to lawmakers who are not completely educated in the technical aspects of the field in which legislation is considered [ibid.:29, his emphasis].

Interestingly enough, this detection of the technological challenges to CI legislation made by Spindel (1968) went largely unnoticed by the occasional academic works on the subject at a time when very few, if any, scholars were considering the full potential of the merging of electronic telephony and digital microprocessors. The subject would eventually be overlooked only to resurface at the beginning of the 1990s, when it constituted the cornerstone of the legislative drive that eventually led to CALEA and RIPA in the US and the UK respectively.

More political and sociological, rather than technical, interpretations of CI are provided in a number of academic works –often too brief and not always directly relevant– such as those of Donner (1980), Theoharis (1978), Joy & Wright (1974) and Navasky & Lewin (1973). The latter two works were published or produced prior to the realisation of the full extent of the Watergate affair, an event that sparked relative concern on the part of American academia over the politics of CI. Consequently, both Navasky & Lewin (1973) and Joy & Wright (1974) tend to confirm, rather than depart from, the earlier findings of Dash *et al.* (1959)[32]. Indeed, the significance of the Watergate affair as an

[31] Bernard (Bernie) B. Spindel was a prominent New York private investigator specialising in CI techniques. During his career he appeared as an expert witness in more than 100 court cases involving CI, often testifying against law enforcement and other US state institutions practising CI.

[32] Characteristically, Navasky & Lewin's (1973) conclusions appear to be in total agreement with those of Dash *et al.* (1959): "(1) the number of federal wiretapping and bugging devices installed without court authorisation is substantially greater that the executive branch has led the public to believe; (2) the average duration of such devices is many times longer than the average duration of court-approved devices; (3) as a result, the total amount of federal electronic eavesdropping without

invigorating force in academic discourses on CI can be witnessed in the works on the subject that emerged after the public disclosure of, and Congressional investigation on, the affair. In the pages of works such as those of Donner (1980) and Theoharis (1978), the mysticism behind CI and the state institutions which practice it withers away. This change of paradigm allows the writers to engage in powerful critical theory that does not need to resort to speculation in order to question the secretive intelligence fortresses of modern America. Simply quoting the congressional reports on Watergate is more than sufficient to severely assault the apparent democratic deficiency that facilitated the unlawful practice of CI by the US intelligence apparatus throughout the Cold War:

> too many people have been spied upon by too many Government agencies and [too] much information has been collected. The Government has often undertaken the secret surveillance of citizens on the basis of their political beliefs, even when those beliefs posed no threat of violence or illegal acts on the behalf of a foreign power. The Government, operating [...] through [...] intrusive techniques such as wiretaps, microphone 'bugs', surreptitious mail opening and break-ins, has swept in vast amounts of information about the personal lives, views and associations of American citizens [...]. The surveillance which we investigated was not only vastly excessive in breadth [...], but was also often conducted by illegal or improper means [. These are] domestic intelligence activities [that] threaten to undermine our democratic society and fundamentally alter its nature [USSSCSGORIA 1976a:1, 5, 12, ctd in Theoharis 1978:110][33].

Against the gravity of such dramatic Congressional accusations, and shocking revelations ranging from the FBI's COINTELPRO[34] program to an impressive array of US Army programs of surveillance[35], US academic texts on CI became less hesitant in openly dismissing official state rhetoric on surveillance or even in directly accusing intelligence agencies of evading legal supervision like common criminals. Writing for the ACLU, Donner (1980) forcefully asserts that US intelligence officials "routinely resort [...] to lying, deception, plausible denial, and related arts to escape detection or,

---

permission far exceeds the eavesdropping with judicial approval; (4) there is strong reason to doubt the validity of the repeated public assurances by the Justice Department that it fully complies with the 1968 congressional standards before installing any tap or bug without a court order; (5) despite the [D]epartment's assertions to the contrary, there is an absence of well-defined procedures which would promote compliance with the statutory standards and permit meaningful congressional scrutiny of this extraordinary executive activity" (Navasky & Lewin 1973:298-299).

[33] Athan G. Theoharis is another American academic who, like Samuel Dash, was involved with (and even testified before) the U.S. Senate Select Committee on Presidential Campaign Activities (a.k.a. the Senate Watergate Committee).

[34] COINTELPRO, which stands for COunter INTELligence PROgrams, is the codename of a series of complex FBI operations aiming to neutralise domestic political dissidents. These operations reached their peak between 1956-1971. For a detailed analysis of COINTELPRO see http://www.cointel.org.

[35] As challenged in Laird v Tatum 408 US 1 (1972).

on higher levels, responsibility" (ibid.:24). Such accusations, stated in writing and put forth with such self-assuredness, were totally absent from academic or popular writing on CI in the US prior to the Watergate affair.

This drastic change of attitude in public perceptions of CI prepared the ground for a new generation of scholars –though, again, limited in numbers– who carried research over to the threshold of the twentieth century. Two of those, Diffie & Landau (1998) recently produced *Privacy on the Line: The Politics of Wiretapping and Encryption*, a long-awaited text that somewhat bridged the analytical gap created by the absence of detailed works on CI following the work of Dash *et al.* (1959). Rather intriguingly, *Privacy on the Line* represents a clear case in which the legal and political controversy of digital encryption, which flared up during the 1990s, led researchers[36] back to the largely neglected issue of domestic CI[37]. In the book, the roots of the digital encryption debate are traced back to domestic CI practices, thus slowly revealing the profound lack of political and sociological research on the subject.

The writers make full use of the hindsight in producing CI research, not only after the Watergate affair, but also after the formal termination of the Cold War, at a period when many of the unlawful CI practices of US intelligence agencies have been publicly admitted to and have even resulted in the imposition of considerable punitive fines against federal intelligence agencies[38]. Thus, the answer to the question of whether CI has been systematically used by state agencies to abuse the civil liberties of citizens is no more a matter of speculation:

> [d]espite strictures to prevent abuses, the US government has invaded citizens' privacy many times over the last 50 years, in many different political situations, targeting individuals and political groups [...]. Sometimes invasion of privacy has been government policy; sometimes a breach has occurred because an individual within the government misappropriated collected information [Diffie & Landau 1998:148].

J. Edgar Hoover's FBI policies are criticised as the prototype mould in which such civil

[36] And, in the case of Whitfield Diffie, the inventor of public key cryptography himself.

[37] "[Wiretapp]ing would be nearly irrelevant to the central subject of this book –cryptography and secure telecommunications– were it not for the fact that bugs and wiretaps are inseparably intertwined in law and jurisprudence and named by one collective term: 'electronic surveillance'" (Diffie & Landau 1998:153).

[38] The reference here is to *Socialist Workers Party v Attorney General of the United States*, 73 Civ. 3160, 1986, in which the plaintiff was awarded a total sum of $263,500 in damages for violations of the constitutional rights of its members (through various means, including the systematic abuse of CI methods) by the FBI, over a period of 25 years; see the collection of articles in Jayko (ed.) 1988.

rights abuses were institutionally shaped[39]. Indeed, Diffie & Landau's (1998) analysis largely reflects the relevant literature in elevating such criticism to the point of directing it against government policy as a whole: "[t]he history of the last five decades", they write, "shows that attacks on privacy are not an anomaly. When government has the power to invade privacy, abuses occur" (ibid.:164).

2.2.0. Broader Contexts in the Literature.

As demonstrated in previous sections of this chapter, the bibliographical starvation that stigmatises research literature on CI can be said to border on famine. Yet, thankfully, research on CI often enjoys the valuable contributions of the broader research contexts from which it originates and in which it is produced. Arguably, the most crucial among these can be said to be the following segments of the research literature: (a) issues relating to the informational, or knowledge-base, parameter in the administrative infrastructure of contemporary Western nation-states –i.e. bureaucracy; (b) issues relating to the monopolistic nature of the informational practices of contemporary Western nation-states –i.e. secrecy; and (c) issues relating to the panoptic character of administrative apparatuses in contemporary Western nation-states –i.e. surveillance. These segments in the research literature are briefly explored in the remaining sections of this chapter.

2.2.1. Information: The Administrative Basis of State Bureaucracies.

During the second half of the 20th century, Western research on state bureaucracy has been largely guided by two fundamental ideological shifts. The first such shift signifies a departure from –primarily Marxist– interpretations of state bureaucracy as a unified bourgeois stratum which exercises the advantages of technical superiority against a technically incompetent civil society (Marx & Engels 1977:10; Michels 1915) [40]. This has led to the largely shared view of state bureaucracies as "essentially polyarchic" (Giddens 1985:4) and multifaceted structures, which neither systematically favour nor impose the interests of the state upon the citizenry (Perez-Diaz 1978:77). Rather, their existence is seen as a platform of negotiation and exchange between state and civil society. This, in turn, often gives state bureaucracies a political dynamic that runs

[39] "Hoover remained firmly in power through eight presidencies and 48 years. His long tenure as director is now recognised as a period during which the FBI routinely engaged in the sort of widespread political surveillance usually associated with totalitarian regimes" (Diffie & Landau 1996:164).

[40] See also Lenin's conception of bureaucracy, as explained in Olin-Wright 1978:208ff.

counter to the interests of both state and civil society, thus allowing them to acquire relative autonomy from both (Lefort 1986:90; Ellul 1965:259; Etzioni-Halevy 1983:87).

The second ideological shift is signified by the introduction of the concepts of knowledge and information as vital parameters of bureaucratic function. Max Weber's profound conclusion that "bureaucratic administration means fundamentally the exercise of control on the basis of knowledge" (Weber 1968:26)[41] has been further articulated and advanced by a number of scholars whose works consistently promote the definition of state bureaucracy as "the application of knowledge by political means" (Apter 1965:316-7). American political scientist Karl W. Deutsch (1963) was the first to make explicit and elaborate references to information as the currency of state governing:

> [g]overnments, that is, political systems or networks of decision and control, are dependent on [the] process of communications [.... T]he dependence of all governments [is] upon the processing of information [Deutsch 1963:145].

He was soon followed by others: Mouzelis (1967) described bureaucratic administration as "control through knowing" (ibid.:39); Meynard (1968:20) and Etzioni-Halevy (1983) asserted that the increasing complexity of large nation states commands that "political decisions are based increasingly on expert technical knowledge" (ibid.:58); Giddens (1985) elaborated on the "expansion of the 'documentary' activities" (ibid.:172) of Western nation states throughout the 20th century; even Foucault (1977) noted that modern state administrations in the West seek "to form a body of knowledge about individuals [...], rather than to employ the ostentatious signs of sovereignty" (ibid.:220)[42].

2.2.2. Information Secrecy as a Bureaucratic Value.

According to the orthodox Marxist thesis, the informational base of state bureaucracy is not by itself a reactionary element in the machinery of government. Rather its restrictive and monopolistic character tends to subvert popular power (Perez-Diaz 1978:78). In other words, it is the monopolistic nature of the informational practices of state

[41] An earlier, though less eloquent, connection between bureaucracy and information was produced in 1895 by Gaetano Mosca, who described state administrators as a "knowledge-holding class" (Mosca 1939:111).

[42] It was around the same time that theorists such as Douglas (1970), Bell (1967) and Galbraith (1967) proposed what they saw as the centrality of the role of "codified theoretical knowledge" (Bell 1967:16) in social and economic growth, a phenomenon leading to a form of society in which "information is the legitimate basis of action" (Douglas 1970:15).

bureaucracies, their pattern of secrecy, which sets them apart from civil society:

> [t]he general spirit of the bureaucracy is the secret, the mystery, preserved inwardly by means of the hierarchy and externally as a closed corporation [Marx & Engels 1977:47; see also Lefort 1986:93].

This viewpoint largely informed the British literature on bureaucracy during the late 1970s and early 1980s. It also interacted with a vocal 'freedom of information' movement, which called for a higher degree of popular access to governmental documents, including those of the secret services. Apart from affirming Marx's view of secrecy as "the bureaucratic law of survival", as Thompson (1976:40) characteristically put it, a number of British scholars challenged official explanations which justified governmental secrecy as an essential and unavoidable feature of a sound national security policy:

> [m]ost government secrets are kept from the public for reasons that have nothing to do with national defence and one of the most important of these reasons is simply the convenience of those in power [Michael 1979:5].

Instead, a viewpoint was projected, which analysed bureaucratic secrecy as a conscious political effort to marginalise popular participation in the inner workings of government and to decrease the vulnerability of administrative power to citizen oversight (Michael 1979:9; Wilson 1984:13). A model of bureaucracy was thus proposed where secrecy was to the parliamentary state what constraint was to the totalitarian regime, namely a force that generated and maintained the relations of power (Leigh 1980:ix) while guaranteeing extravagant amounts of political pleasure to those in possession of power:

> [p]art of the joy of being at the top is being in the charmed circle of the few 'in the know' and civil servants say that this is what they miss most when they retire. Releasing information reduces the extent to which they are exclusively in the know [Chapman Pincher, ctd in Wilson 1984:19].

The short-lived 'freedom of information' movement managed to briefly unify the scattered elements of the British progressive community under the single-issue banner of challenging governmental secrecy. Though ultimately unable to seriously disrupt the informational practices of British state bureaucracies, its political principles managed to survive over the years and resurface in the 1990s to form of the ideological foundations of the 'cyber-liberties' movement.

In the US literature, the issue of bureaucratic secrecy, though it arose from a different

political premise, has also been strongly emphasised[43]. The US Freedom of Information Act (FOIA), as well as the unique legislative and congressional oversight of the US intelligence community, have often acted as alleviators of political tension formed over the issue of popular access to bureaucratic information (Lowenthal 2000:133). Thus, in the US, calls for reforming the informational practices of state bureaucracies have been both less extensive and less combative than those voiced in the UK[44].

The issue, however, occupying American scholars working on government secrecy has been the apparent total breakdown of the aforementioned alleviating forces during large parts of US history, such as the periods of McCarthyism and Hooverism and including the period leading to the Watergate affair. The primary question that has been guiding research in the field has been *how was it that manifestly unlawful civil rights abuses were institutionalised despite the existence of an elaborate and rigid legal framework of oversight and accountability*? Most of the responses generated in the literature are centred on the theme of the 'national Cold War consensus'. The latter usually signifies a broad and far-reaching attitude of concurrence, built on anti-Sovietism and anti-communism. This attitude characterised American society throughout the 1950s and 1960s and was largely manifested in overwhelming support for an aggressive foreign policy of containment of the Soviet Union and its allies and for an equally aggressive domestic policy of neutralisation of leftist political agents operating within the US:

> secret agencies [...] operated for some twenty-five years with few questioning their operations. The national consensus, founded on anti-communism and developed by periodic crises, supported a bipartisan foreign policy and a strong, active presidency. The president's authority to defend the national security was generally accepted, and his instruments went unquestioned. Few reporters, legislators, or citizens ever attempted to strip away the veil of secrecy, to expose the spy bureaus to review and the few that tried failed. In this, the intelligence agencies enjoyed the license of the secret police in a dictatorship: they could spy on others without concern for others reviewing them. Th[is] enabled the covert bureaus to operate outside the normal checks and balances of the constitutional system and above the law itself [Halperin *et. al* 1977:222; see also Olmsted 1996:4, 59ff; Johnson 1988:8].

The concept of the national cold war consensus, which ended with the controversial US

[43] The UK's 'freedom of information' sister movement in the US probably reached its peak in 1973, with the Government Secrecy conference in New York City, NY; see Dorsen & Gillers 1974.

[44] There are, of course, examples in the US literature of more militant approaches to the issue of bureaucratic secrecy, such as the works of Wise (1973) and Demac (1984). These are, however, fairly

involvement in the Vietnamese and Cambodian conflicts, has directed researchers to a rather sophisticated model of bureaucratic secrecy. According to this model, bureaucratic secrecy in the US has been an organic phenomenon that largely evolved out of the permissive social contract guiding relations between state and civil society in post-war America. Even when the Watergate and Church committee investigations brought down some of the fortresslike structures of secrecy surrounding US intelligence institutions, most Americans appeared disturbed, rather than angry, argues Kathryn Olmsted (1996):

> the intelligence investigations [...] forced Americans to acknowledge that their country had tried to kill foreign people. Because this knowledge was very painful, many Americans, including members of Congress, refused to accept it. Secrecy, as journalist Taylor Branch has said, 'protects the American people from grisly facts at variance with their self image' [[45] ibid.:7].

To a large extent, Olmsted (1996) continues, the Watergate and Church committee investigations failed to achieve a long-lasting effect on the structures and culture of the US administrative establishment. This failure was not because the findings were not caustic or shocking enough, but because, ultimately, American civil society did not wish to be exposed to the revelations of those investigations (ibid.:7ff).

2.2.3. Bureaucracies as Panopitc Apparatuses.

Significant segments of the vivid debate of the informational nature of contemporary nation states are also to be found in the literature on surveillance, the production of which has reached unprecedented heights in recent years. The foundations of the debate were set in 1973 by James B. Rule's groundbreaking work entitled *Private Lives and Public Surveillance*. The theories and assertions that emerged from that work eventually fuelled a whole range of scholarly production, from Foucault's psycho-esoteric explications on the nature of discipline in modern societies (Foucault 1977:111, 1983:296-297) to Giddens' critical writings on the functional characteristics of contemporary nation states (Giddens 1985:177ff).

The significance of Rule's (1973) work rests on the fact that, through his elaborate study on the micro-techniques of bureaucratic information collection and amassment, he

---

atypical of the broader spectrum of the relevant literature, which is, on the whole, less self-assertive and more mediative in nature (see for instance Shils 1974; Rozell 1994; Lowenthal 2000:184ff).

[45] This quote is from Branch 1976:126.

successfully extricated the notion of surveillance, which he then considered as a facilitative aspect of social development. In other words, for the first time in the history of sociological analysis, surveillance was explained, not necessarily as the outcome of the bureaucratic imperatives of organised societies, but rather as one of their preconditions. Surveillance was therefore analysed as a potentially generating force behind organised forms of social coexistence:

> one may expect new means of control to emerge to ensure compliance among the participants in [...] larger scale social units. In many cases it may be difficult to determine whether the growth of a larger scale social unit spurred the development of new means of control. But one may be certain that the increase in social scale will not proceed any faster than the development of means for assuring compliance within the social structures. And the development of those techniques will, where mass clienteles are involved, entail growth in the capacity of mass surveillance and control [Rule 1973:308].

The above observation is more important than it may initially appear. Through it, Rule (1973) accomplished two significant achievements: firstly, he successfully transferred the notion of surveillance from the realm of the technical to the realm of the sociological[46]; secondly, by virtue of this very transfer, he cleansed his analytical models of surveillance from technological-deterministic elements, which insist on viewing social models of surveillance as necessarily technological phenomena.

When considering the latter of these two achievements, it is indeed difficult to resist viewing some of the more recent works on surveillance as scholarly steps backwards, rather than forwards. Some of the more recent scholars exploring the field seem to aspire, albeit often unknowingly, less to Rule's structuralist conceptions and more to Jacques Ellul's techno-deterministic views on social change, characteristically embodied in the following quote:

> [t]his entry of technology means control over all the persons involved, all the powers, all the decisions and changes [.... T]echnology imposes its own law on the different social organisations, disturbing fundamentally what is thought to be permanent [Ellul 1989:134-135].

In accordance with Ellul, Gandy (1989) proposes a view of surveillance in modern societies that is in essence technologically driven and technologically achieved. Not only are its functional horizons and social effects determined by its technological

sophistication, but its very nature, its very guiding principles are inherently technological. Thus the interconnection between computerisation and digital telecommunications networks constitutes "the material force in the new technology of surveillance" (ibid.:63), which "by definition [...] dramatically increase[s] the bureaucratic advantage" (ibid.:46, 62).

A more balanced approach is offered by Lyon (1994), who, on the one hand, recognises that the introduction of new technologies of surveillance could potentially erode already established civil liberties and freedoms by altering the technical balance of modern societies in favour of highly organised bureaucracies (ibid.:41)[47]. Yet, on the other hand, he goes to great pains to clarify that

> [t]he fact that information technology provides the instrument or means of this strengthened surveillance does not mean that surveillance capacity is an outcome of technological pressures. They play a part [...], but within the broader context of political, economic and cultural processes that give them their chance [Lyon 1994:88].

Even in the case of intelligence services where, according to Lyon (1994), advances in technology are often highly instrumental in the construction of the overall context of work practices (ibid.:114), technology's role is primarily constructed through a series of social and political decisions by agents who wish to see national security grow dependent on new technology (ibid.:116)[48].

This social constructivist view of technological development allows Lyon (1994) to proceed in Rule's (1973) scholarly footsteps in yet another explanative parameter: Lyon (1994) insists on viewing surveillance as a multifaceted social phenomenon, whose technical nature is often decisively adapted to suit a variety of political climates:

> surveillance society has more than one face. It may be viewed either from the perspective of social control or from that of social participation. The administrative machinery constructed during the nineteenth century can be understood both as a negative phenomenon [...] or, more positively, as a means of ensuring that equal treatment is meted out to all citizens

---

[46] "[T]he underlying questions concerning the growth of mass surveillance to date, and the future which it portends, are inherently sociological" (Rule 1973:34).

[47] In Giddens' (1985) words, this balance is eventually tilted "because the mnemonic and distributional advantages [that digital technology] allows over purely oral culture are immense" (ibid.:172ff).

[48] A similar approach is followed by Klerks (1995), who, in the context of practical law enforcement work in the Netherlands, analyses technology as a priority-setting parameter, which is fed into feasibility estimates, thus influencing the everyday practices of police officers (ibid:108).

[Lyon 1994:31[49]].

Thus, as a technological construct, surveillance is explained in reference to a constant process of definition and redefinition which occurs throughout history and is moulded by, as well as moulding, the formation of the socio-political landscape in which it operates. Numerous scholars agree that surveillance can be, often simultaneously, the technical infrastructure of hierarchical repression or the facilitative machinery of democratic discourse –the provider of universal citizenship of the welfare state:

> [s]urveillance could act as a limitation upon arbitrary state action, could regulate the exercise of state power and organise the structure of 'real rights' which dominated classes might win [Poulantzas 1978:76-91; see also Lyon 1994:32; Dandeker 1990:108; Holton & Turner 1989:23; Giddens 1985:309].

The above is seen to be applicable particularly in the context of capitalist social relations. The 'rights of the individual', the vital ideological cornerstone of free-market doctrines, precisely requires that the individual and his or her needs are differentiated from those of the mass citizenship by a highly penetrative and highly perceptive –a panoptic– governing bureaucracy. Hence, "the *panoptic sort*" (Gandy 1993:1) is in essence the "all-seeing eye of *the difference machine that guides the global capitalist system*" (ibid., emphasis added). Indeed, the connection, or lack thereof, between surveillance and capitalism is a theme repeatedly pursued in the relevant literature. One view, primarily expressed by Giddens (1985) and Dandeker (1990), refuses to view surveillance as the latest link in a causal reaction involving the capitalist enterprise. The latter characteristically asserts that the view of bureaucratic surveillance as one of the tentacles of the capitalist octopus should be exchanged for a more flexible analytical model, which explains surveillance as an institutional dimension of contemporary large-scale social structures –an "administrative means of reproducing a social system of rule" (Dandeker 1990:viii, 38). Another view has been expressed by Gandy, who sees surveillance as an important source of economic growth in post-industrial capitalism:

> the real source of growth in both the information work force and the development of information technologies is not to be found in any transformed consumer demand, but in the continually expanding surveillance requirements of multinational corporate enterprise [Gandy 1989:61].

---

[49] Lyon (1994) is here in agreement with Rule (1973), who states that "[i]mprovements in the apparatus of surveillance and control may work to secure the position of social units whose existence would otherwise be tenuous" (ibid.:306).

Yet, despite such differences, few scholars offer substantial objections to the assertion that those of us living in the information societies of late capitalism are gradually being subjected to unprecedented levels of surveillance practices by both state and corporate bureaucracies. Indeed, it is the unprecedented level of bureaucratic organisation that makes the information society possible, which has allowed for an equally unprecedented overpowering of surveillance capabilities and uses. As the infrastructure of the information society expands to become proportional to the entire spectrum of human activities and desires, so does surveillance. For Giddens (1985), it is through surveillance that administrative power "increasingly enters into the minutiae of daily life[, scanning even] the most intimate personal actions and relationships" (ibid.:309). Others pose the question of whether it is practically possible to escape surveillance in the context of the information society –and decide that it is not: the era of the information society is the age of over-penetrating bureaucracy, to such an extent that simply "to participate in modern society is to be under electronic surveillance" (Lyon 1994:4; see also Gandy 1989:61; Dandeker 1990:2).

It is this lack of choice, symbolised by the panoptic character of surveillance in the information society, which leads many writers to ultimately dismiss the exercise of surveillance as an inherently reactionary and evil sociotechnical construct,

> an antidemocratic system of control that cannot be transformed because it can serve no purpose other than that for which it was designed: the rationalisation and control of the human existence [Gandy 1993:227].

Less deterministic accounts, such as those of Lyon (1994:68), Wilson (1984:97) and even Rule (1973), usually express a similar degree of moral frustration over surveillance, a frustration that often goes beyond the legal shortcomings that may surround its use[50], or the possibly repressive political motives of its users. There is a sense in which the exercise of surveillance is seen as morally objectionable in and of itself, even when put toward goals that may reinforce democratic values, such as equality and citizenship:

> [m]y position is simply that these practices are sufficiently undesirable in themselves and in certain of their potential consequences that we would do well to curtail them wherever possible. This judgement applies even in cases where systems operate with justice and on behalf of highly desirable purposes. Indeed, the development of popularly-supported 'just' systems of surveillance strikes me as more worrying in the long run than

[50] Which do not go unnoticed in the literature; see for instance Gandy 1989:61; Wilson 1988:52, 66.

> those against which popular sentiment is capable of being aroused [Rule 1973:350].

The above position describes something of the essence of the domestic CI debate: both proponents and opponents of communications surveillance depart from premises that derive straight from principle, while paying little, if any, attention to the particular outcomes and effects of the practice. Proponents view CI as morally bound with the exercise of justice through government. Opponents view it as immorally bound with the exercise of injustice through government. Consequently, statistical, social and technical analysis is usually provided to justify, rather than to challenge, the ideological axioms informing scholarly or popular attitudes. Yet it is this striking impasse which authenticates the genuineness of this fascinating argument that, despite its obscurity, lies right at the very core of notions of the limits of power, democracy and freedom in the information society.

2.4.0. Summary

In the US and the UK the literature on domestic CI is extremely limited and often polarised. The reasons for this are both evident and understandable: the lack of basic information from credible sources –or, indeed, sources at all– as well as the considerable political sensitivity of the subject, have largely isolated CI and related issues from the realm of academic exploration. Despite these unfavourable conditions, some academic and popular accounts of CI and related issues have managed to provide interesting analytical frameworks, in which a number of crucial issues have been highlighted, challenged or reinforced. One of them has been the overall secrecy and lack of democratic accountability of intelligence institutions. This, in connection with a number of high-profile political episodes involving the illegal use of CI –such as Watergate– have not done much to improve the negative perceptions, as well as the considerable scepticism over CI which permeate the relevant literature. This scepticism is by no means groundless. Nevertheless, it may be necessary for it to be methodologically penetrated by research, in order for the entirety of this admittedly complex issue to be fully uncovered.

Chapter Three

Some Considerations of Method

3.0.0. Introduction.

The absence of any systematic academic debate on domestic CI –highlighted in the preceding chapter– had a peculiar impact on this study. Depending on the occasion, it was either a discouraging or an encouraging force. It denied me the luxury of basing my research hypotheses on a solid mountain of thoroughly documented material; the absence of such a mountain, or hill for that matter, was often a time a dispiriting constraint. On the other hand, this very absence proved to be the primary motivating force behind the operational persistence that guided my research through its four-year duration.

Ultimately, it was this critical absence in academic research on the subject that largely shaped the methodological framework of this study. In the following sections of this chapter, the particular features of this methodological framework will be explained with reference to the decision-making processes that brought them about. Prior to engaging in a discussion of the interviews, there follow a number of observations about the general nature of this research, as well as a brief consideration of primary and secondary sources of information which were made use of at various stages of the project.

3.0.1. The General Nature of the Research.

When I commenced this project, in October 1997, I did it with the understanding that the

research involved would be essentially a matter of construction –a process of constant adding and building upon a firm and secure bedrock of prescribed assumptions. I was mistaken. Looking back over the past four years, it is clear that this research has been primarily a process of demolishing and remodelling the infrastructure of initial hypotheses and expectations, followed by brief, refreshing periods of erecting unforeseen new structures upon these –equally unexpected– remodelled foundations.

A particularly illustrative example of the above was the gradual realisation of the limited extent and analytical shallowness of the literature on CI, which, on the whole, proved too outdated and too scant to adequately address contemporary developments in the digital telecommunications environment. It was only following this realisation that the significance of interviews as primary sources of original information began to emerge. Consequently, it was not until late 1998 that I was able to form a clear set of criteria and goals for potential interviews.

Gradual, too, was the construction and evaluation of a set of selection criteria for the interviews. My initial view of CALEA and RIPA was that of two critical pieces of legislation destined for implementation by state agencies over a docile and subdued industry. It was only later that I comprehended the full extent of the polemical attitude of the US and UK industries, as well their central position in the digital CI debate[1]. Initially, I was also unaware of the absence of industry, as well as of law enforcement and intelligence from the relevant literature. Eventually, this absence effectively directed my research toward concentrating on industry and law enforcement interviewees (see section 3.3.3).

I do not wish to hide the fact that my initial view on interviews was negative. The comparative nature of the project meant that a potential interview schedule would have to cover two countries, a requirement that would undoubtedly contribute to the logistical complexity of the project. Furthermore, the inherently covert nature of the subject under research meant that detecting knowledgeable insiders and persuading them to divulge some of their knowledge would be an arduous task.

These reservations proved to be unfounded. Even though, statistically, only about 15 per cent of institutions and individuals approached with interviewing requests replied

[1] Described in sections 7.4.2; 7.4.3; and 7.4.4.

affirmatively, the overall number of 113 requests yielded the respectable total of 21 interviewees, everyone of whom possessed unmatched theoretical, legislative or practical knowledge of the field. As I began to network with respondents, I was referred by them to other individuals, who in turn often referred me to more people. Eventually, my initial reservations about contacting people unknown to me with the request to interview them 'for the sake of academic research' was replaced by an eagerness to speak to as many knowledgeable insiders as possible in my effort to address the intriguing questions guiding this project. In fact, I believe that had I not ran out of time and financial resources, I would still be pursuing further interviews.

Also unexpected was the willingness of some interviewees to meet me and speak to me. True, many questions, especially those of a more investigative nature, were either tactically or abruptly avoided by respondents during interviews; but many other equally inquisitive questions were addressed with clarity and honesty that took me by surprise. A former Special Branch Officer described how UK law enforcement and intelligence agents abuse CI during 'fishing operations' (Int12:406ff); a veteran British Telcom engineer admitted the existence of illegal CI practices, facilitated through the intimate personal relationships between CSPs and local law enforcement constabularies (Int03:401-408); while a BellSouth security official and CALEA project manager openly confirmed the FBI's unofficial efforts to dictate the technical and quantitative specifications of digital CI (Int21:29-34) –a form of pressure which has been deemed illegal by US law (see section 6.3.0); most unexpectedly of all, a source requesting anonymity forwarded me information on Oratory interception technology, whose existence has never been confirmed in academic or popular literature on the subject of CI. (see sections 3.2.1; 8.4.2)[2]. Further information was supplied in print and digital format by a number of interviewees (see section 3.2.3).

3.0.2. The Comparative Element.

There is nothing particularly novel about the comparison between the UK and US CI experiences, on which this research is methodologically based. The similarities in the digital features of the two nations' telecommunications infrastructure are accompanied

[2] It is important to state here that not all interviewees requested anonymity. The application of anonymity to all interviews –with the exception of Bowden (2000) and Akdeniz (2000), who declined anonymity– was my own decision, reached after deliberation with my supervisors. The latter are the only people, apart from me, who have access to the names of all interviewees.

by a broadly similar regulatory environment, which has in turn caused the emergence of a series of largely identical legislative steps to restore state-sponsored CI capabilities (see section 8.1.0). Recently, this parallel status has been noted by a number of academic observers (Sutter 2001; Walker 2001) and has even been remarked upon by industry representatives involved in the digital CI debate (Clayton et al. 2000).

These identical features aside, the choice of the UK experience as a case study for this project was further promoted by the immediacy of the RIPA debate –which is still unfolding as this thesis is being finalised for submission. The choice of the US experience was justified by the unique size of the nation's telecommunications sector, as well as by the chronological novelty of CALEA, which was the first-ever attempt by a government to address the CI parameter in the digital telecommunications environment.

3.1.0. Secondary Sources of Information.

In light of the academic silence over domestic CI, both in the UK and the US, it is no surprise that, in the course of this project, strictly academic publications on the subject proved to be very limited sources of information. Regrettably, there is nothing unique or abnormal about this. In what is the most recent and, arguably, most sound academic work in English on domestic CI, Diffie & Landau's *Privacy on the Line* (1998), the same trend is observed: of the 431 references of non-technical nature cited by the authors, not more than 28 –approximately 6.5 per cent– originate from academia and of those only 15 were produced in the 1990s (Diffie & Landau 1998:287-317).

3.1.1. Reliance on Government Information Sources.

This present study mirrors Diffie & Landau's (1998) work in yet another methodological parameter, namely in the heavy secondary source reliance on information provided by governmental bodies. To claim that governmental agencies in the US and the UK provide open-access information resources on the subject of domestic CI would be gravely misleading. As will be explained in a later section[3], in both countries the most significant segments of CI policy negotiation between government actors, or between them and industry actors, have taken place behind closed doors –and continue to do so today. Yet it is also true that, in many instances, the amount of information that is made

[3] See sections 7.5.1; and 7.5.2.

publicly available by governmental agencies can often be surprisingly abundant[4]. A characteristic case in point in the UK has been the debate on electronic CI as it relates to digital encryption: detailed and unrestricted access reports have been produced by State officials for the use of British MPs –such as, for instance, POST 1998– which have often braved to hint the appearance of imminent legislation proposals many months before the latter were even acknowledged by government ministers and press secretaries[5]. In other instances, House of Commons records –Hansard– and Parliamentary committee reports can penetrate into the inner workings of the Cabinet, even to the point of disclosing controversial inter-governmental disputes. For example, a revealing 1997 report produced by the bipartisan House of Commons Select Committee on Trade and Industry expressed its members' fears that the UK government might attempt to introduce

> key escrow, key recovery or related measures [...] through the back door as a result of the government's participation in electronic commerce [HCSCTI 1997:2].

In the US, instances of useful –from a research viewpoint– information publicised by government agencies are anything but rare. Indeed, the majority of that information tends to originate from the very governmental institutions that are said to be the most secretive, such as the FBI and the Central Intelligence Agency (CIA). The vast majority of Congressional or other Federal testimonies by FBI officials, often heavily loaded with detailed technical information (Yarbrough 1999; Morris 1999), are publicly available in their entirety and attest to the significant changes in the FBI's culture of secrecy over the past decade or so[6]. In more than one instance during the course of this research, information that local US law enforcement officials were absolutely not prepared to disclose, was acquired directly from declassified or unrestricted CIA documents (such as by Burton 1994).

---

[4] It is entirely possible, of course, that the declassified or non-secret information on CI made available by governmental agencies is minuscule, when compared with the amount of information that remains restricted. It is indeed difficult, or even impossible, to make valid conclusions on the extent of informational openness of governmental institutions when it is often the extent of secrecy itself that is the greatest secret.

[5] See, for instance, the aforementioned POST 1998: "[m]any anticipate that the DTI's revised proposals (expected imminently) will reflect these [encryption] concerns and provide for a more voluntary regime with less demanding conditions for private key escrow" (ibid.:4).

[6] When it comes to CALEA, the FBI even publishes a monthly newsletter on the subject, which is freely available to all who access its web site, or through subscription (Hildebrand 2000).

3.1.2. Reliance on Industry Information Sources.

Indeed, public officials in the US proved altogether much more accessible and less suspicious and secretive than corporate officials when it came to discussing the inner features and implications of CALEA. This, however, does not mean that the industry's official reports and statements on the subject proved to be of lesser value than governmental documents. The latter provided useful windows into the nature of the relationship between the telecommunications industry and law enforcement in the US. Perhaps more importantly, such documents often assisted in determining exactly where the policy line was drawn, demarcating that which was negotiable from that which was not or that which was requested or demanded from that which was freely offered on the table of negotiations between industry and government actors. In other cases, industry documents proved useful in highlighting the industry's efforts to incorporate proposed changes in domestic CI into the sector's overall policy agenda[7]. This was particularly he case in the UK, where the lack of co-operation between industry actors appears to have often prevented their input from being funnelled into the legislation (Anonymous 1999).

3.1.3. Reliance on NGO Information Sources.

Throughout the course of this project, relevant reports and statements issued by Non-Governmental Organisations (NGOs), including civil liberties advocates, were credited with an interpretative significance that was often denied to them by governmental and industry actors on both sides of the Atlantic. Nevertheless, the advocative nature of such material meant that it had to be taken into consideration to the extent in which it offered analytical insight into relevant political and legislative developments which went beyond the simple reiteration of arguments based upon *a priori* reasoning. This proved to be the case as often as it did not. On balance, however, it would be fair to claim that reasoning based on principle, rather than on social and technical analysis and calculation, was by no means monopolised by NGO reports on domestic CI. Considerable segments of the relevant literature produced by government, law enforcement and even industry bodies built their arguments on emotional and highly unsubstantiated rhetoric that rendered them problematic from the point of view of academic research, though regrettably not

[7] "The nation's local telephone companies have worked side by side with law enforcement for many years to provide them with surveillance technology and access to caller information. We take this responsibility very seriously and are committed to assisting law enforcement agencies with crime prevention and detection measures" [USTA 1998:1].

from the point of view of policy formation[8].

3.1.4. Reliance on the Popular and Specialised Press.

Finally –not in order of significance– the reliance of this project upon relevant reporting in the popular and specialised press, both in its printed and on-line formats, has been constant and substantial. This was indeed a necessary requirement, given the ongoing technological and legislative developments in the field of domestic CI during the past 4 years.

3.2.0. Primary Sources of Information.

The primary sources of information that were acquired and analysed in the course of this research can be sorted into four distinct categories based on their format: (a) correspondence between concerned actors and myself; (b) copies of unpublished written communications between third parties; (c) copies of unpublished, restricted, confidential or leaked government or industry reports; and (d) interviews with concerned actors. These source formats shall now be discussed in the order in which they have been listed.

3.2.1. Personal Correspondence.

During the early stages of this research, written personal communications were primarily used, along with the telephone, to facilitate the arrangement of interviews with concerned actors. Later, however, it became clear that this form of communications would be, in itself, a source of primary information. In a number of cases –usually involving law enforcement officials in the UK– postal correspondence was implicitly used by potential interviewees as a means of avoiding direct face-to-face contact, in an attempt to avoid detailed discussions of domestic CI. Their insistence on responding only to questions put to them in writing subsequently served them as a strict and effective mechanism of controlling the amount of information they were willing to release to me during our exchanges[9].

Electronic mail –often in encrypted form– was used as a means of extracting primary

---

[8] For a discussion of emotionalism and unsubstantiated rhetoric in CI policy negotiation see section 7.5.9.

[9] All this correspondence is in my possession and has been filed in my records.

information in two particular ways: firstly, it was used to communicate with interviewees, following interview exchanges, in order to clarify points made during the interviews and to request further information on particular topics that were of interest to this research. Most interviewees who were contacted in such a manner did provide further information. Secondly, electronic mail was used to extract information from individuals who were either located too far away or were too busy to facilitate face-to-face or telephonic interviews with me.

Encrypted electronic mail proved to be a means of receiving relevant information from individuals who were willing to share it with me in a manner that would secure their privacy. It was indeed through encrypted electronic mail that I acquired some of the more sensitive information regarding domestic CI, including an interesting list of telecommunications companies that agreed to offer their consent in favour of CALEA in return for government contracts for CALEA-required hardware and software. Perhaps more importantly, it was by means of encrypted electronic mail that I received information regarding Oratory, a NSA-sponsored CI technology, whose existence has yet to be confirmed in academic literature on the subject[10].

3.2.2. Correspondence Between Third Parties.

In two separate instances, I acquired copies of written communications between third parties –usually, though not always, between organisations and agencies. The first set consists of correspondence between UK law enforcement officials and the Department of Trade and Industry (DTI) concerning the Interception of Communications Act (IOCA) and the RIP Bill. I do not believe that these documents are in any way restricted, but it is my impression that they have yet to be formally released to the public. The second set of communications consists of correspondence exchanged between US industry officials and a number of industry associations concerning US encryption technology and legislation. I believe that these documents have since been released to the public, though it is my impression that they have yet to find their way into published academic discourse[11].

---

[10] All exchanged emails are in my possession. They have been filed in printed format in my records, with the names of those individuals who wished to remain anonymous removed from the copies.

[11] All copies of the aforementioned correspondence are in my possession and have been filed in my records.

3.2.3. Unpublished, Restricted, Confidential and Leaked Reports.

Telecommunications industry conferences have been significant sources of primary material on RIPA and CALEA. In addition, printouts of a confidential conference presentation for FBI security officials have been acquired, as have two other reports, classified as 'confidential'. These reports were produced for the Electronic Surveillance Technology Section of the FBI (ESTSFBI) by Booz-Allen & Hamilton technology consultants, under their Strategy and Implementation Plan for the FBI's National Infrastructure Protection Centre (NIPC). The plan involves "addressing the Bureau's law enforcement, counterintelligence and counter-terrorism responsibilities" (Booz-Allen & Hamilton 1999)[12]. I have also made use of one UK government agency report –originally classified 'restricted'– produced by the NCIS Deputy Director-General Roger Gaspar (Gaspar 2000), and leaked to the Observer newspaper by an unnamed source (Ahmed 2000).

3.3.0. The Decision to Interview.

As was mentioned in section 3.0.0 above, it was the critical absence of the subject of domestic CI from academic research that largely shaped the methodological framework of this study. The decision to proceed with interviews and use them as primary sources of data was partly an outcome of this critical absence. Even in instances were enlightening documents were available –as, for example, in the case of the IOCA consultation period in the UK, or in the series of lawsuits by CSPs against the FBI in the US– interviews with key participants could potentially offer valuable research handles. These interviews had the potential to shed cognitive light on the inner political mentalities and the judgement and belief systems of actors who helped determine certain policy resolutions by ruling out alternatives which they deemed harmful to their respective interests. Parallel to that ran the need to unveil and explore any traces of conflict between actors –a need rarely catered to in existing documentary evidence. It was those seeds of controversy, uncovered during many of the interviews, which helped me visualise the enormous sea of complexity delineating the tiny islets of concrete policy which have slowly emerged from its depths.

---

[12] The two reports (Booz-Allen & Hamilton 1997; Booz-Allen & Hamilton undated) were received on two 3½ floppy disks, in html hyper-document format. I have printed the documents, which are in my possession and have been filed in my records.

Input was also sought from those telecommunications professionals whose working culture and practices are in the epicentre of the technological and legislative tremors that have been rocking the field of telecommunications security and policing for almost a decade. In retrospect, it appears that, no matter how profound or illuminating they have been, governmental, corporate or legal documents were unable to provide this research with the degree of cognitive penetration achieved in even the most deficient and mundane of the interviews conducted.

My decision to conduct interviews was reinforced by an encouraging stream of bibliographic tradition of sociological research into police cultures, based on interviewing[13]. British writer James McClure's fascinating account of the San Diego, CA, Police Department, entitled *Cop World* (1984), was based on several months' worth of recorded interviews from police officers. Despite its somewhat casual character –or due to it, one might argue– the book succeeds in shedding light into some of the more intimate thoughts of law enforcement officers about their role in American society. One officer characteristically remarked in one of the interviews

> [a] guy says, "I got arrested for drunk driving –you can't tell me that a cop doesn't get drunk!". And he's right. In a way, being a cop makes you a hypocritical person (smiles). I write very few tickets and I lock up very few drunks [ctd in McClure 1984:147].

Other similar works based on interviewing include David J. Smith's exemplary research on *Police and People in London*, especially vol. III, *A Survey of Police Officers* (1983). It was based on representative questionnaire sampling and a series of informal interviews of senior police officers (Smith 1983:3). Mike Seabrook's book entitled *Coppers* (1987) also provided an inside view of the British police and an oral history of police culture based largely on non-attributable interviews.

Ultimately, the motivating principle behind the decision to interview was the following: wherever there is a deficiency of readily available sources of information, the researcher's duty is not to shy away from the field, but rather to facilitate its demystification –to break into its concealed territory– by *creating* sources of vital information.

---

[13] I have been unable to locate any instances of interview-based sociological or political research into telecommunications-oriented social groups or individuals.

3.3.1. Creating Information Resources.

Even prior to commencing the buildup of my interviewing schedule, I was aware that I had chosen to enter a number of socio-political domains which are traditionally hostile to academic inspection, especially of the more investigative kind. Not many years have passed since the time when even mundane research interest in domestic CI attracted the intense gaze of suspicious security officials. The notorious ABC[14] trials in the UK were indeed rare incidents representing the unfortunate culmination of such suspicious attitudes. However, most of the classic examples of critical research into elements of domestic CI –such as Bunyan's *The Political Police in Britain* (1976) or Theoharis' *Spying on Americans* (1978)– did not come about without their writers having to combat the overwhelming appearance of red signals and red tape in various government offices.

Times have changed, though regrettably not that much. In one particularly memorable instance, I was advised by an official close to Sir Roy Cameron, Chief Constable of Edinburgh's Lothian and Borders Police, not to pursue interviewing anyone from his office on the subject of wiretapping because the first thing the Constabulary would do after receiving my request would be to "place a tap on your line to find out what on earth you're on about". In another instance, after instinctively rejecting my request to interview members of her department, a junior Tennessee Bureau of Investigation (TBI) officer demanded to see my identification so as to report our conversation to her superiors as a "contact with a foreign national".

Regrettably, researchers who endeavour to step into politically sensitive government territories are all too familiar with such responses. In his study of the US Military Academy at West Point, Spencer (1982) notes that there are five basic reasons why bureaucratic elites attempt to bar social researchers from having access to the inner workings of their institutions:

> bureaucratic rigidity and threat to personal careers; the potential threat to the power of their institution; the threat to the subjective reality constructs of their institution; the problem of the legitimacy of the researcher; and the problem of exchange [Spencer 1982:24],

[14] The ABC affair was named after the surname initials of the two journalists and one soldier (Crispin Aubrey, Duncan Campbell and John Berry) arrested in the late 1970s under the UK Official Secrets Act. The affair is outlined in Aubrey 1998 and discussed in depth in Aubrey 1981.

namely the idea that the institution will not have anything to gain in return for opening its doors to the researcher. All of these institutional barriers made their disheartening appearance throughout the course of this project. They left their unmistakable mark in the large number of negative responses I received from potential interviewees, and in the much larger numbers of letters of request and follow-up telephone messages that went completely unanswered by individuals and organisations whom I tried to approach. Yet, even when I was able to finally meet volunteering interviewees, the fear of the possibility that their names and remarks might be used in this thesis to criticise the institutions for which they worked made many remarkably cautious in voicing their opinions. As a senior BT Security Officer put it toward the end of his interview:

> I mean, these are my personal opinions and, you know, I'd rather they didn't come back and land on my head [...]. I'm not paranoid about it, it's just...I just, you know, I say that because...so you understood, you know, if anything...if anything did go wrong [laughs]. I'm just saying that to let you know [British Telecom Security Officer, Int07:267-270[15]].

On the whole, requests to discuss domestic CI were turned down by the vast majority of law enforcement and other government and industry officials contacted in the UK and the US, including officials from the NCIS, the US-based International Y2K Co-operation Centre, the US Department of Justice (USDoJ) and the National Institute of Standards and Technology (NIST). The reply to my letter of request from Peter F. Maddison, Assistant Chief Constable of Hertfordshire Constabulary, was typical of most law enforcement responses I received. "I regret that I am unable to take part in such an interview", he wrote, and continued:

> [a]s I am sure you understand, the subject is extremely sensitive and has many complex issues affecting Police Forces and other Law Enforcement Agencies within the United Kingdom [Maddison 2000].

Ultimately, interviews were conducted and a respectable amount of new data was collected with the generous help of insiders –a clear indication that times are indeed beginning to change. According to one interviewee, a British telecommunications security lobbyist and former Special Branch investigator, this research was conducted in a rather timely manner. When asked about whether there was public transparency in the areas of co-operation between law enforcement and CSPs, he remarked:

> [r]easonably so. I mean, you've only got to go to the NCIS web site to see how open that organisation is. And certainly, I mean [...], in the time frame of the last two to three years increasingly more open. [P]rior to that no –prior to that behind close doors. And you wouldn't even discuss it; [...] you wouldn't even admit its existence half the time. But that [...] has changed [Int12:451-455].

Thus far, however, such winds of change seem to be leaving unaffected the corporate telecommunications culture. Prior to commencing my pursuit of interviewees among the CSP industry, I had been made aware of the traditional secretiveness, which is part of the history of corporate telecommunications, through such works as Fitzgerald & Leopold's *Stranger on the Line* (1987) and Sampson's *The Sovereign State* (1973). Yet I doubt whether anything could have prepared me for the extent of corporate secrecy which, in many instances, hampered my attempts to initiate direct lines of communication with CSPs on both sides of the Atlantic.

In the case of the UK, notable refusals to even consider my request for interviewing came from, among others, UUNet Ltd, the Internet Service Providers' Association (ISPA) and the Federation of the Electronics Industry (FEI) –all of them corporate actors that have been deeply involved in domestic CI legislation. Particularly disappointing were the numbers of corporate telecommunications security officers, who agreed to be interviewed after meeting me during a telecommunications conference in London, only to write back a few days later and express regret at their superiors' refusal to grant them permission to talk about the issue to an outsider.

In the case of the US, corporate secrecy appeared to be almost omnipresent. Close to 50 letters of request for interviews were sent out to various CSP corporations and industry associations, 37 of which were followed up with telephone calls. Only one request, sent to the Organisation for the Promotion and Advancement of Small Telecommunications Companies (OPASTCO), resulted in an interview.

Academic literature on interviewing and related matters is often permeated by the belief that, though acquiring permission to interview the people to whom one sets out to speak is not an easy task, one will find the vast majority of potential interviewees to be co-operative, altruistic and willing to share their knowledge with academic researchers. In

---

[15] In this citation, "Int07" refers to 'Interview 07', whereas the numbers "267-270" refer to the particular lines of text in the transcript of the interview.

one of his classic books on specialised interviewing techniques, L.A. Dexter professes his belief that, though there are no statistics on the subject,

> the proportion [of those researchers] who succeed in getting needed interviews is almost certainly much higher than the proportion [of those] who fail [Dexter 1970:29].

The experience of this research confirms Dexter's statement in that a respectable number of interviews was, eventually, amassed; but it refutes it in the sense that the vast majority of the 113 public and corporate individuals and organisations who were approached with interview requests, rejected them or, more often, simply ignored them.

3.3.2. On the Use of Informants.

The term *informant* is used by social anthropologists to signify an individual who either is a member of, or has direct access to, a particular research subject of a project, and who engages into a rather close relationship with the researcher, thus helping the latter achieve "cognitive learning" (Paul 1953:443-444) of the issue under examination. Looking back on the course of this project, it is now clear to me that I achieved this particular research rapport with three individuals, one of whom is located in the UK and two in the US. None of the three was my acquaintance prior to the initiation of my quest for interviews. What is more, none of the three were specifically requested to become informants for the purposes of this research. Our special relationship was triggered firstly by their unconditional agreement to be interviewed once approached by me and, secondly, by their remarkable frankness and openness expressed during their interviews on matters generally regarded to be extremely sensitive in nature. Our relationship was carried through by the frequent exchange of electronic mail messages and telephone calls following our interviewing sessions.

At no instance did any of the three supply me with information which I consider to be of a particularly clandestine or classified nature, though two of them supplied me with information that rarely finds its way into the public domain. The two a retired Special Branch Communications Intelligence officer, and Counterintelligence Unit officer of the US Special Forces, serving on inactive duty while at the end of his long career. The remaining informant was an FBI Special Agent and Unit Chief of the Bureau's CALEA Implementation Section's Telecommunications Industry Liaison Unit. At no point did he provide me with any classified or even restricted information. His informant status stems

from his remarkable frankness during our very long interview, as well as from his willingness to provide me with extremely valuable resources and documents –a willingness that dramatically counters the stereotypical prism through which many view the contemporary FBI.

3.3.3. Practical Considerations.

The lack of openness that has for many decades permeated the subject of domestic CI has heavily contributed to the element of unpredictability that characterises the field. Inevitably, this very element of unpredictability dominated interviewing considerations from an early stage: undoubtedly, permissions for interviews would be extremely difficult to acquire in both the US and the UK. Law enforcement agencies are certainly not used to discussing CI with outsiders, and neither are CSPs who, due to the extreme competitiveness of their industry, are some of the most PR-conscious corporations of late capitalism. This difficulty rendered interview target numbers increasingly irrelevant. Fifty interviews with tight-lipped experts could prove worthless, while one long, frank interview with a knowledgeable insider eager to provide vital information could translate to page after page of invaluable data.

The financial element played a crucial role in the arrangement of the project's interviewing features along pragmatic lines. The sum of £1,320, generously provided by the Economic and Social Research Council as part of its Research and Training Support Grant, was used to fund all 21 interview trips on both sides of the Atlantic. Limited funds had to be spent wisely and such considerations were important influences upon decisions relating to interviews. They were instrumental, for instance, in my decision to concentrate less on government advisers or legislators and civil liberties organisations and more on members of law enforcement organisations and industry officials. This was based on the fact that the opinions of the latter –especially industry officials– are inexcusably absent from the scant literature; the opinions of the former, however, are either discernible in numerous governmental documents, reports and testimonies on the subject of CI or, as in the case of civil liberties advocates, they are exposed in more on-line and off-line activist publications than one could possibly be able to monitor.

Inevitably, the list of completed interviews reflects this decision: out of the 21 conducted during this project, no less than 14 were of members of the industry or of its various

associations; five were of current or former members of law enforcement and intelligence bodies; while only two were of executive members of civil liberties organisations. No interviews of civil servants or other government officials were conducted, though some were unsuccessfully pursued. This unbalanced composition is obviously less than ideal, though it is somewhat inversely proportionate to the visibility of these socio-political groupings in the literature.

Ultimately, I find that it is with a feeling of achievement that I gaze upon the list of completed interviews: if an inexperienced PhD candidate can find ways to peak into the traditionally concealed territories of law enforcement, intelligence and corporate administrations, then surely these areas, as well as those of elected and appointed government officials, should not prove difficult for more proficient researchers to approach.

3.3.4. Selecting Interviewees

Having chosen to focus on potential interviewees from the telecommunications industry and law enforcement, I decided to scan through relevant government documents, extracting names of individuals, organisations and companies who had responded to governmental calls for consultation on various matters around IOCA, the RIP Bill and CALEA. A minority of those contacted in this manner agreed to be interviewed. They included a former BT Engineer, whose input on the IOCA consultation paper was particularly dismissive. They also included one of BT's numerous Regulatory Affairs Officers, who has for many years been the Company's regulatory liaison with law enforcement agencies in Britain and abroad[16].

Particularly welcome were acceptances from individuals representing industry associations –and thus speaking on behalf of extensive corporate memberships. Among these were a Regulation Officer working for the London Internet Exchange, Ltd, with many years' experience in dealing with the Home Office and the DTI on matters of CI; the Chief Executive Officer of Telecommunications UK Fraud Forum (TUFF) –the UK industry's primary official liaison with law enforcement and intelligence; and the Technical Director of OPASTCO, an organisation that has for many years been deeply upset with the financial burden that CALEA has placed on smaller CSPs, located

[16] Since our interview he has resigned from BT and has moved on to work for another UK CSP.

primarily in the rural regions of the US. This latter respondent was also responsible for referring me to two other representatives of collective industry bodies. These were a former lobbyist and one of the few US experts on the telecommunication industry's government relations; and the Director of the National Services Planning sector of the United States Telecommunications Industry Association USTA , the largest and arguably most important corporate telecommunications body in the world.

These are all knowledgeable individuals representing corporate bodies whose input and views on domestic CI have often been as important as those of government legislative experts. Yet, legislation and lobbying aside, their first hand experience of wiretapping is extremely limited. Therefore, another group of interviewees was used to fill in this gap. They included the aforementioned[17] FBI Special Agent, who specialises in telephonic surveillance and has been involved –both as an interception technician and project supervisor– in thousands of the Bureau's domestic and international CI projects. In 1992 he became the first FBI agent to indicate in a report the dramatic reduction in interception ability that US law enforcement organisations would face as a result of the digitisation of telecommunications. Finally, this group of interviewees included one of the very few BT security officers in charge for many years of conducting authorised domestic CI on behalf of UK law enforcement agencies; and an Emergency Communications technician employed by a law enforcement organisation, which, in compliance with his request, will remain undisclosed in the context of this project.

It was with the help of this latter respondent that I finally managed to enter what proved to be a most hermetically concealed research area: that of the US telecommunications industry. He personally referred me to two of his industry liaison contacts, BellSouth's CALEA Attorney and CALEA Project Manager. One other industry interviewee, a Fraud Control Manager for a large UK CSP, was referred to me by TUFF's Chief Executive Officer.

Additionally, three more industry interviewees were contacts I developed while networking in the UK; these were a Fraud Control Manager and law enforcement liaison for a large UK CSP; the Chief Executive Officer of a large UK Internet service provider (ISP); and a UK-based Fraud Liaison Officer working for a multinational CSP. She was kind enough to allow me to audit her telephone exchanges with various law enforcement

[17] See section 3.3.2.

officers during part of a day's work[18].

In the UK, two of the civil liberties executive members approached with interview requests were willing and able to be interviewed. They were Caspar Bowden, Director of the London-based Foundation for Information Policy Research (FIPR) –one of the most vocal and visible civil libertarian groups in the legislative negotiation over domestic CI in the UK; and Yaman Akdeniz, Director of Leeds University's Cyber-Rights & Cyber-Liberties UK, the organisation which first published evidence of CI-related clandestine negotiations between law enforcement agencies and CSPs in the UK, in February of 1998 (ISPA 1998).

3.4.0. Evaluating the Interview Method.

The character of the interviews conducted during this project has been crucially shaped by one basic factor: information scarcity. The generally limited information on domestic CI meant that, more often than not, the person in charge during interviews –that is, the person generally defining the limits of disclosure– was the person in possession of scarce information –namely the interviewee. I do not necessarily consider this feature to have been negative; to some extent, it is the very nature of a semi-structured elite interview to be an exercise in uncovering the specialised knowledge of the interviewee. As Dexter (1970) admits:

> in standardised interviewing [...] the investigator defines the question and the problem; he [or she] is only looking for the answers within the bounds set by his [or her] presuppositions. In elite interviewing [...], however, the investigator is willing, and often eager to let the interviewee teach him [or her] what the problem, the question, the situation, is –to the limits, of course, of the interviewer's ability to perceive relationships to his [or her] basic problems, whatever these may be [Dexter 1970:5-6].

I admit that part of my eagerness was, of course, simulated. I wanted interviewees to aspire to their own expertise as they were being interviewed, and thus I avoided influencing or curtailing them by expressing detailed knowledge of their fields of specialisation. Rightly or wrongly, I felt that going about it otherwise might cause interviewees to guard their responses. That was deceiving as much as it was genuine: it denoted my determination to interview in an unassuming manner –to confirm as much as

[18] The interview with this respondent, whom I met at a London conference, was conducted in Greek which is our native language. The interview was transcribed by me in Greek and only the parts used in this thesis were translated into English.

possible by taking for granted as little as I could.

This semi-structured and non-standardised style of interviewing does not imply, however, that the interviews lacked a clearly defined and, indeed, commonly shared anatomy. Although all interview questionnaires were carefully customised to suit the information assets of each particular respondent[19], all 21 interviewees were called to reply to a largely similar set of basic questions which corresponded to the project's core research interests. This common central theme of questions was linked according to logical procession and categorised according to subject matters, so as to allow me maximum topic control, as well as the initiative of directing the course of the interview within specified time limits –usually not in excess of 75 minutes.

In almost every interview, a pressing issue was how to pose questions that were considerably investigative in style without putting interviewees on the defensive. The most convenient way around this problem, which I chose to adopt, was to camouflage such questions under generous amounts of tactful phrasing. Thus the question "*are you afraid that the government will try to undermine you and your interests once you turn your eyes away from the issues at stake?*" became: "*to what extent has the element of trust been present in the negotiations between CSPs and the government in regards to CALEA?*"; while the question "*do CSPs usually undermine the law by honouring unauthorised CI requests from law enforcement?*" was smoothed out to read "*during your career, and according to your knowledge, have CSPs always been served with warrants prior to assisting law enforcement with CI?*". Rather surprisingly, the answer to the latter question was not always affirmative, which can be taken to mean that, despite their de-clawing, many of the questions asked did actually serve the investigative spirit that brought them into existence. Yet, asking "*how would you describe the relations between law enforcement or intelligence agencies and CSPs in Britain today?*" is certainly not the same as asking "*do law enforcement and intelligence agencies have secret dealings with CSPs behind the backs of both customers and citizens?*". The decision I took in making research questions appear rather harmless was essentially a compromise. Yet I would like to think that, on balance, it uncovered more information than would have been generated if straightforward and tactless questions resulted in a repeated breakdown of communications between respondents and myself.

---

[19] A sample of an interview questionnaire is provided in Appendix 1.

This manner of disguising the sharpness of questions under a veil of silk-like phrasing involved one disadvantage –namely it made some questions appear heavily loaded. For instance, the question: "*is it your opinion that, in the long run, CALEA will help reduce, or even eliminate, unlawful CI by third parties, including law enforcement and intelligence?*", presupposes a number of rather controversial suggestions –namely that unlawful CI by law enforcement does take place today and that it might take a long time for the phenomenon to be brought under control. It is indeed true that "any question contains and supplies information, at the same time as eliciting and requesting information" (Dillon 1990:99). Yet, when it comes to controversial themes, such as domestic CI, interview questions that appear to assume as facts heavily disputed suggestions might disturb the interviewer. This did occur during my interview with one particular individual (Int06), who repeatedly stressed that he thought he was being asked a series of heavily loaded questions. That interview could have developed more favourably, from a research standpoint, had I managed to unload some of the controversial assumptions contained by a handful of questions.

My decision to approach members of law enforcement and intelligence agencies, as well as members of the telecommunications industry and also civil liberties advocates, was largely due to my belief that this project would have a lot to gain by being receptive to the views of different actors concerned about the same socio-political event –namely, the drafting and implementation of RIPA and CALEA. I expected to detect elements of the complexity of that event by uncovering differential stances and disputes between actors. Thankfully, that was achieved: the traditional lines of dispute between law enforcement and intelligence, the industry and the civil liberties lobby were pushed aside as more unexpected and interesting disputes appeared –between CSPs and manufacturers of telecommunications hardware, between large and small CSPs, between metropolitan and rural law enforcement departments, between intelligence lobbies and government legislators and so forth. Yet, the limited volume of specialised interviews meant that few of these aforementioned complexities were explored in detail. For instance, no members of smaller law enforcement departments –either here or in the US– agreed to be interviewed; nor did any representatives of hardware-based telecommunications corporations, such as Nortel Networks, or Sysco, even though both their US headquarters and UK subsidiaries were approached. Further persistence and extra financial resources would have assisted in bridging some of the gaps created by these

deficiencies. More effort to acquire and exercise both should have been made prior to, and during, the research stage.

Perhaps the most intricate of the methodological questions, which I have silently been considering throughout the course of this project, revolves around the element of truth and its relationship to the interviews conducted: how do I know whether interview respondents have been telling me the truth? In other words, to what extent has truth been revealed in the interviews? It is not a question that I have taken lightly and I have particularly tried to filter out what may appear to be convenient responses such as relativist conceptions of the truth. Attractive though the concept of relativism often seems to me, it is one that I frequently choose to brush aside when I sense that it emerges at the expense of more inconvenient answers. I do not, therefore, necessarily wish to dispute that the truth of an issue under research, though usually complex and multitarian, is a value to which the researcher can aspire without essentially compromising the sophistication and analytical quality of his or her research.

The most satisfactory response I have been able to provide involves disputing the legitimacy of the initial question. The latter implies two matters: firstly, that research interviews are conducted with the aim of reaching the truth and, secondly, that research interviews are somehow able of reaching the truth. None of these assumptions are particularly valid: I have not for one moment assumed that my interviewees' statements disclose anything other than what *they* consider to be the truth or, at most, the parts of truth that they consider suitable for public consumption. For instance, it was clear to me from speaking to a number of intelligence agents that they honestly viewed domestic CI as a practice that safeguards national security. One can argue that this may not be so in reality, but it is nevertheless a true opinion held by individual and institutional actors who have shaped UK and US privacy legislation in very real and concrete ways. In other words, the interview aims –and has the ability to– uncover the personal perception of the respondent, rather than the essence of the truth of the matter, whatever that may be. In their consideration of this very same issue, Dean & Foote-Whyte (1970) wisely remark that the respondent's statements

> represent merely the perception of the [respondent], filtered and modified by his [or her] cognitive and emotional reactions and reported through his [or her] personal verbal usages [Dean & Foote-White 1970:120].

Not only does this mean that that which is revealed in an interview is purely the view of

events according to the respondent, but also that, strictly speaking, this particular view should be solely attributed to the respondent's state of mind during that particular interview. "Under other circumstances", the authors continue, "what [the respondent] reveals to us may be much different" (ibid.). I was repeatedly alerted to this intriguing phenomenon during my interview expeditions: often the information disclosed to me by a particular respondent during his or her interview was totally different from what the very same respondent confessed to me afterwards, while buying me a drink at the local bar or pub. One particular individual, a corporate telecommunications lobbyist, who had spent large segments of his recorded interview trying to convince me that it was his company's honour to be assisting law enforcement's wiretapping requests, told me afterwards that

> on record all of us will tell you that we're happy to do this as a service to the community and all that. But nobody likes doing it –snooping on customers' phone calls. It's bad ethics and it's really bad PR –I'll tell you that right now.

There were, of course, times when informants supplied me with information that was meant to be particularly descriptive and objective. A case that comes to mind was the information I received in regards to the NSA's aforementioned[20] Oratory technology. Never has the existence of Oratory been confirmed in academic or popular literature on the subject of CI. The information I have been supplied is a description of the technology by an individual who used it for a number of counterintelligence surveillance operations. This data could lead one to the conclusion that this technology is in existence and in use today. Is this information true? I personally believe so, but have specifically avoided presenting it as such in this thesis. I have rather considered it as evidence, a small segment of information pertaining to a larger quest for transparency. And I wish to stress that it is as such that it should be read.

3.5.0. Summary.

The findings of this project were based on a variety of primary and secondary documentary sources, as well as on a series of interviews. The former included personal correspondence, government and industry reports and additional unpublished, restricted and confidential government-produced material that was passed on to me by insiders.

[20] In section 3.2.1.

Interviews were conducted in the US and the UK over a period of several months and were used to generate most of the primary data on which this project is based. In evaluating the interviews, it should be admitted that many decisions, which were taken in order to allow me to overcome certain methodological barriers, ultimately created as many problems as they solved: for instance, an ESRC monetary award that allowed me to conduct the interviews also placed strict financial limits on how many interview expeditions I could conduct, which, in turn, let to priority-setting; in another example, the tactful phrasing of investigative questions asked during interviews generated more information from respondents who might otherwise have been put on the defensive, but compromised the investigative principles of this project. The search for truth and its meaning for the interviewing process has been yet another issue discussed in this section. Ultimately, it is, I believe, possible to challenge the premises of the question of whether truth was extracted during the interviews, without necessarily resorting to a convenient form of relativism.

Part II
EXPLORING THE HISTORICAL FRAMEWORK

Chapter Four

The Government and Telecommunications in Historical Context

4.0.0. Introduction

Scottish-born American inventor Alexander Graham Bell was issued with a copyright certificate for his telephone by the US Patent Office on the morning of February 17, 1876. Reportedly, he managed to patent his new apparatus less than two hours before another inventor, Elisha Gray, of Western Union –then the dominant telegraphy company in the nation–, would have patented a remarkably similar innovation (Martin 1991:1). This somewhat amusing account is indicative of the early history of the telephone –a history marked by the dynamic, and often chaotic, combination of a variety of technical, commercial, political and ideological interests displayed by a variety of actors.

In this chapter I wish to illuminate some of the more vital elements of that complex history with reference to the relationship between modern governments and telephony. In the interests of coherence, I have partitioned the chapter into two primary sections. The first section is concerned with the early attitudes of UK governmental bodies and agencies over the appearance of the telephone network in British territories. In it, there will be attempts to enrich current historical understanding of the state's reaction to the new technology, which appears to be somewhat reductionistic and focuses almost exclusively on the financial parameters of that reaction. These attempts will be carried out by introducing a number of social and political parameters to the debate.

The second section is concerned with the early attitudes of US governmental bodies over the appearance of telephony in the nation. This section will be rather briefer, as historical understanding of the subject, as reflected in the relevant literature, appears to be less deterministic and more aware of the social and political elements feeding into governmental decisions and actions.

4.1.0. Messenger Boys and Telephones in the UK.

Ironically, Bell found it considerably easier to invent and perfect his telephone than to convince governments around the world that the new invention was worth taking an interest in. British civil servants proved to be a particularly unyielding lot. In September 1877, after being exposed to Bell's presentation of the new communications instrument, the Post Office's Engineer-in-Chief issued an official report against the idea, stating –among other arguments– that the potential of the practical use of the telephone in Britain and the Empire was extremely limited (Robertson 1947:11). Equally unimpressed by the presentation was the Post Office's Chief Civil Servant, who made his opinions known in numerous reports to the British government (Perry 1977:72). The latter repeatedly turned down the opportunity to purchase Bell's British patent (Aronson 1977:16), and it was instead bought by a group of private entrepreneurs who sponsored the construction and operation of the nation's first telephone network in London, established in 1878[1].

The operation of the country's first telephone network had little, if any, effect on the negative attitudes against telephony among many government circles: in 1879, the new Engineer-in-Chief of the Post Office, W.H. Preece, reported to the House of Commons that he could see no point in further extending the telephone network. In one of his report's characteristic passages, Preece justified his perception of the telephone as a socially useless contraption by resorting to that omnipresent feature of British social life –class:

> I fancy the descriptions we get of its use in America are a little exaggerated, though there are conditions in America which necessitate the use of such instruments more than here. Here we have a super-abundance of messengers, errand boys and things of that kind [...]. The absence of servants has compelled Americans to adopt communication

[1] The entrepreneurs, who operated under the instructions of the Bell Telephone Company, established the first telephone company ever to operate in Britain, the Telephone Company Ltd. –later renamed National Telephone Company, Ltd.– on June 14, 1878. It was officially registered with a capital of £100,000 (Robertson 1947:12).

> systems for domestic purposes. Few have worked at the telephone much more than I have. I have one in my office, but more for show. If I want to send a message, I use a sounder or employ a boy to take it [ctd in Dilts 1914:11].

Despite the amusing shortsightedness of Preece's words, there is an important sense in which the Post Office's refusal to secure the exclusive rights to the manufacturing and operating of telephones is not indicative of the seriousness with which the British government took the new telecommunications medium. Discernible among the records of debates at the time is a small, but influential, group of government policy makers who absolutely rejected the notion that a British telephone system could be developed outside the boundaries of state control (Perry 1977:83; Perry 1992:149ff). Accordingly, their examination of the dynamics of the new invention was swift and detailed. Perry (1977) reports that

> the telephone was taken very seriously by the Post Office [...]. By March 1877, [before Bell approached the British government,] the Post Office had already instructed its chief engineer to report on the capabilities and practical utility of the telephone. Studies were made of telephone technology in America [Perry 1977:72-73].

This seriousness was reflected in the decision of the Post Office to assume the crucial role of the agent of the Telephone Company, Ltd., in return for receiving 40 per cent of the company's gross rental income (ibid.:1977:73). Indeed, the case can be made that the initial decision to abstain from direct control over the technology was anything but an outcome of ignorance or heedlessness. Rather, the government, already in control of the nationwide telegraph and postal networks, preferred to lie in wait, while allowing private investors to attempt to overcome early impediments to telephonic development. Such impediments included, for instance, the problem of voice amplification over distances and also geophysical threats to transmission cables. In the absence of a well-funded engineering effort of considerable magnitude, these problems could have seriously hindered the future of telephony. Even as late as 1890, when the *London Times* and the *Economist* were frequently running editorials urging a government takeover of the telephone system, the Treasury Department's Senior Civil Servant ruled out any such possibility in the immediate future, insisting that

> my Lords are not prepared to embark upon another enterprise gigantic in itself, while the developments it might lead to are beyond their powers of prediction [R. Bundle, June 27, 1890, ctd in Perry 1977:88].

Ultimately, it would seem plausible to suggest that the guiding premise of the British government's early policy toward the telephone was to patiently observe the emergence and initial development of the enterprise "without incurring more than a minimum of direct responsibility" (Robertson 1947:46).

4.1.1. Telephony's Takeover.

The principal legislative safeguard enabling the Post Office of the day to distance itself from early developments in telephony is to be found in the legal precedents of mail and telegraphy nationalisation. In accordance to these, the British government could assume direct and overall control of the telephone system at any point in time, and for whatever reason it saw fit, without being required to seek the industry's permission or approval. The following extract from the minutes of a Treasury Department meeting on April 8, 1899, is indicative of the legislative assurance that the aforementioned precedents had lent government officials:

> [t]he right of the Post Office to establish telephone exchanges and to license persons, companies and other bodies to establish such exchanges (a right explicitly reserved in every license and agreement with the National Telephone Company) will remain intact; and should Her Majesty's government at any time see fit to exercise this right in a manner different from that indicated in this minute, neither the company nor any local authority will have any ground to complain of breach of contract, or want of good faith on the part of the Postmaster General [ctd in Robertson 1947:69].

Rarely, of course, was there anything close to a consensus within the state apparatus over plans for a possible nationalisation of the telephone system. Some in the Treasury regarded nationalisation as the lesser of two evils, the other being fierce competition (ibid.:55-56), while some saw private, or even municipal competition, as a vital element in the successful evolution of the enterprise (Perry 1977:89ff). Even more complex were the constantly shifting positions of influential individuals within the Post Office, many of whom insisted that the telephone had absolutely no future in Britain as a public utility, while, at the same time, actively urging the government to pursue a policy of nationalisation[2].

[2] A case in point was Postmaster General Lord Manners. While passionately claiming that the "the telephone could not be utilised on the public wires in any way" (Perry 1992:147), he insisted that "the matter [of private telephony is] not one in which the Post Office could remain passive" (Perry 1977:73-74).

Yet, despite some intra-governmental disputes, there is little doubt that, by 1880, the small telephony industry community in the British Isles was becoming increasingly uncomfortable over the prospect of a government takeover. The Telegraph Act of 1869[3], the nation's primary telecommunications legislation, permitted little room for speculation: section 4 of the Act entrusted the Postmaster General with the sole right to operate "any apparatus for transmitting messages or other communications by means of electric signals" (ctd in Robertson 1947:23). Rather predictably, in 1880, Crown lawyers successfully sued the National Telephone Company for privately operating a section of the state's electric communications network, namely the telephone network (Robertson 1947:21ff; Canes 1966:9). Following that decision of the High Court, the National Telephone Company as well as a number of smaller, private or municipally controlled companies, were subjected to a set of strict regulatory guidelines[4]. Furthermore, an annual 10 per cent gross income royalty was required as payment –on top of income taxes– to the Post Office (Robertson 1947:26, 45; Perry 1977:82). Finally, operational licenses

> became due [to expire] at the end of thirty-one years, i.e. on 31 January 1912; the Post Office reserved the right to purchase the system at the end of the 10th, 17th, or 24th year; what would happen if, in 1912, the Post Office refused to renew the license was not mentioned [Robertson 1947: 26].

The National Telephone Company held out until 1912, when it was bought over by the Post Office (Perry 1977:90). Additionally, after nationalisation, only 13 of the 60 municipalities that expressed an interest to develop their own, locally controlled telephone systems, were granted licenses. Of the six[5] that ultimately proceeded to use them, only the Hull Telephone Company managed to survive (ibid.).

4.1.2. Challenging the Motives Behind Nationalisation.

On the surface, the government's takeover of the telephone system constitutes one of the most paradoxical events in the history of British economic policy. Late 19th and early

[3] Th e 1869 Act was itself a protégé of a series of regulatory settings in the area of telecommunications, which included the Telegraphy Acts of 1854, 1863 and 1868, as well as a number of statutes dating back to 1837, 1710 and 1657, facilitating state control over postal services.

[4] Discussed in section 4.1.2.

[5] Those were Glasgow, Brighton, Hull, Swansea, Portsmouth, and Tunbridge Wells. According to Perry (1977:89), "[i]n retrospect, the movement for municipal exchange systems was a smokescreen that only delayed the inevitable creation of a single system under Post Office management".

20th centuries marked an era permeated by an overwhelming support among governing elites for open markets, free from substantial state intervention. It was a time when virtually all of Britain's pillar industries, namely coal, bronze, steel and shipbuilding, were the products and emblems of free capitalist enterprise. It was within that political and economic context that, first the telegraph, in 1869, and then the telephone, in 1912, were completely taken over by the state. They were the first nationalisation projects in British history and indeed, economic historians inform us, signified the first use of the term 'nationalisation' (Tivey 1966:65). Even more remarkably, both projects were conceived, designed and implemented by a series of Conservative and Liberal administrations (Barry 1965:177). It is perhaps this latter element that lies behind the striking lack of academic interest on these instances of nationalisation. Perry (1992) makes the insightful claim that the roots of this phenomenon are to be found in

> the tendency of some historians to link nationalisation with Labour party history and, therefore, to dismiss those cases of government expansion which are not part of that tradition [Perry 1992:86][6].

The few historians who have examined British governmental attitudes toward telecommunications have, for the most part, been all too willing to distinguish between two primary motives behind the decision to nationalise. On the one side, the argument goes, the government aimed to provide an efficient, standardised telephone system under unity of control, thus accommodating the communication needs of businesses as well as the public (Pierce 1977:192; Perry 1977:83-84). Additionally, it is often claimed that government and Post Office executives interpreted the rise of the telephone as a threat to their telegraphy business and decided therefore to nationalise telephony so as to make up for any lost revenue (Robertson 1947:22, 45, 87; Perry 1977:82).

The first supposed motive behind nationalisation appears to be, quite simply, a fallacy. As later sections of this chapter will demonstrate, the British government's take-over of telephony was the primary cause of the underdevelopment of telephonic communications as well as of the systematic discrimination and exclusion of non-business users, which lasted until the late 1960s.

The second motive corresponds to a greater degree with reality. It is difficult and,

[6] I have had the opportunity to confirm this in my own literature research on the subject. Of the works on British nationalisation considered classics by contemporary economists, none even acknowledges the telegraphy and telephony nationalisation projects (see Blank 1973; Brooke 1991; Chick 1991; Middlemas 1986; Rollins 1992).

indeed, undesirable to overlook the interest of the British government and the Post Office in safeguarding the dominant status of telegraphy as the major communicative artery of the nation. By 1876, the telegraph network had been in use in Britain for more than 40 years. At that time, there were already over 5,000 telegraph offices throughout the country and dispatched telegrams exceeded the impressive number of 50 million per year. Equipped with over 200 long-distance submarine cables, which linked London to the furthest corners of the Empire, Britain undisputedly possessed the finest and most efficient communication system in the world (Aronson 1977:16; Perry 1977:75).

Often, government Ministers and Post Office executives did not hesitate in proclaiming their determination to prevent an experimental voice transmission system, promoted by an unknown inventor, from displacing the already time-tested, most profitable, as well as most extensive in terms of use and size, electric communication network on the planet. In one such comment, on March 22, 1893, the Postmaster General, Sir James Fergusson, warned that there was a

> real danger of the valuable public property, the telegraph system, being injured by the extension of this telephone system [.... W]herever the telephone system has been principally developed, there the growth of the telegraph revenue has been checked [...]. If the telephone companies were in communication with all the large towns and sent messages all over the country, undoubtedly the system would to a large extent supersede the telegraphs and consequently largely diminish the telegraph revenue. Therefore, it is [...] essential [...] that the government should have possession of the trunk wires [ctd in Canes 1966:10; Robertson 1947:45].

A few years earlier, his predecessor, Postmaster General Lord Manners had expressed similar opinions on the issue of the coexistence of state-owned and private telephone companies, in a memorandum to the Treasury Department:

> I think you will see that the matter [of private telephony is] not one in which the Post Office could remain passive, for if renters of private wires, on the expiration of their agreements, had applied to have their wires fitted with telephones, and their application had been refused, they would, I need scarcely say, have employed contractors to erect fresh wires, and the Post Office would have had old wires thrown on its hands [ctd in Perry 1977:73-74].

However, argues economist M. Canes (1966:10), the fear that the competition for customers between telephone and telegraph networks might result to a reduction of telegraph revenue for the state did not necessarily have to lead to nationalisation. From an economic standpoint there were many alternative solutions to the government's

concerns, including restrictions on telephone investment, the functional limitation of private telephone enterprises to local distance communication, or even the imposition of high government taxation on the gross income revenue of private telephone companies. Nationalisation was but one of numerous sets of measures that could have adequately safeguarded telegraphy. Canes' argument is furthered in light of telephony's poor financial performance under state control: the initial 1913 surplus of £303,000 had been extinguished by a £100,000 deficit by 1915 (Raine 1920:95). Indeed, positive financial indicators never reappeared during the next 70 years[7].

Ultimately, a lack of logical coherence characterises this argument: if it were the case that the primary motive behind the nationalisation of telephony, in an age of free enterprise, was to safeguard the state's telegraphy revenue, then how are we to explain the nationalisation of telegraphy during the same era? And, if the motive for that was the safeguarding of the state's postal revenue, then how are we to explain the state's postal monopoly? Surely, a solution that would have been much more compatible with the spirit of the times would have facilitated the privatisation of all telecommunications, as well as the provision of a legal framework promoting the development of the sector through free-market competition. This was certainly the case with all large-scale industries of the day. The fact that this did not take place cannot be effortlessly dismissed as an instance of economic inconsistency in the policies of a series of governing administrations of the world's dominant superpower.

An additional motive behind nationalisation, often favoured by historians, focuses on a desire of elements in the British state to safeguard the interests of the public, as well as of business users of the new technology. Privately operated telephonic communications were expensive and inefficient. Thus, the argument goes, by introducing a much-needed unity of control over telephony the government hoped to promote its expansion (Perry 1977:83-4)[8].

This argument, however, appears to be historically unfounded. To begin with,

---

[7] The absence of parliamentary oversight is often blamed for these indicators: "Parliament was unable to see what costs and profits accrued separately to the telephone or telegraph postal services. Bureaucratic procedure dominated the organisation and ministers overseeing the department came and went with unusual rapidity" (Wolmer 1932:14).

[8] According to orthodox economic theory, this argument would fall under the category of social regulation of private enterprises; the latter signifies the type of governmental regulatory intervention which primarily aims to promote public interests that the profit-motivated market appears to be unable to meet voluntarily (Hills 1986:29).

commentators agree that it was the very process of regulatory strangling, imposed by the British government on private telephony following the 1880 decision of the High Courts[9], that was responsible for the technical and administrative inefficiencies of private networks. In London, for instance, no company was allowed to operate further than a radius of five miles from a central point. At the same time, companies were forbidden from constructing trunk lines, erecting poles on, or passing wires over, private or public property, making the practical operation of a telephone system virtually impossible. Hills (1986) has stressed that it was this very

> geographical limitation of these local networks through structural regulation, coupled with recurring threats of nationalisation [that] stimulated local monopoly exploitation, which in turn led to public pressure for nationalisation [Hills 1986:78].

Reportedly, the situation became so desperate that, on June 7, 1895, the principal technical journal of the country, the *London Electrician*, in a dramatic editorial, called for the total abolition of the entire telephone system (Robertson 1947:52). It appears, however, that the striking popular, parliamentary and administrative consensus that allowed for the nationalisation of telephony had been generated by frustration over the inefficiencies of private telephony that the government itself had created.

An examination of the telephone's development in Britain, following the take-over, points to the fact that the decision to nationalise

> was [...] at once short sighted, immature and legalistic. [What is more, t]hat it was established so early in the history of the telephone development in this country was one of the major causes of slow progress over thirty years [Robertson 1947:21].

From the very beginning, governmental administration of the telephone network was so tragically inefficient that the notoriety of the service increased rapidly to unprecedented levels[10]. Political power-struggles in and out of the House of Commons, as well as the bureaucratic use of red tape by Post Office officials, resulted in circumstances that were often farcical. In one such incident, the Post Office refused to purchase telephone

[9] Discussed in the previous section.

[10] Writing less than 8 years after nationalisation, G.E. Raine asserts that "delays and mistakes drive the user [of telephony] to exasperation and sometimes to despair. Its inefficiency is a severe handicap to the business of the country [...]. The outstanding features of telephone control by the state have been the vast increase in the cost of running and also the cost to the user, coupled with a steady deterioration in the quality of the service" (Raine 1920:95).

instruments from private manufacturers, while at the same time refusing to manufacture them itself (ibid.:49)[11]. The frustration of users is detectable in written records of the time. Writing less than a decade following nationalisation, Raine (1920) exclaims that

> [t]hese telephones are so essential to the community and the loss and annoyance that result from this inefficiency are so great, that we may anticipate a resolute movement in favour of their denationalisation [Raine 1920:96].

As far as the Post Office was concerned, telephony was a technology designed for corporate use (Perry 1977:83). During the early decades of the 20th century, business interests were exceptionally influential in determining telephone pricing policy. Thus, it was only in 1915 when the Post Office hesitantly began to consider the gradual abolition of the flat rate pricing system and the adoption of reduced telephone charges for the public, at the expense of business users –a policy which, in Europe and North America, had been brought into force almost two decades earlier (ibid.:91ff, Pool *et al.* 1977:131).

Yet, even that development did not challenge the elitist culture of telephony administrators. Successive generations of sceptical and uninspired Post Office officials stubbornly refused to view the telephone as anything but a luxury that was to serve the business needs of the aristocracy. According to Marvin (1988:101), the class-based exclusiveness of the telephone service constituted a "political priority" for the British government. This was openly expressed at an early stage by no other than the very Postmaster General, A. Morley, who, in a statement before the Commons in 1895 suggested that:

> [...] the telephone could not, and never would be an advantage which could be enjoyed by the large mass of the people [ctd in Marvin 1988: 101][12].

Well into the 20th century, the telephone remained far beyond the reach of the vast majority of the British population: an annual fee of £17 was required for unlimited telephone use in 1920, when a family could hire and maintain a servant on a full-time basis for £20 per year (Robertson 1947:80, 188; Perry 1977:78, 83). Inevitably, in December of that year, less than two per cent of the total population were telephone subscribers (Perry 1977:82).

[11] Ultimately, the technical features of the network were "consistently undermined" by the Treasury's "lack of investment", which "precluded the necessary technological upgrading, while lack of marketing kept usage rates low" (Hills 1986:78).

Combined with the systematic underdevelopment of rural telephony, this situation inevitably resulted in the disastrous retardation of the British telephone system in relation to systems in continental Europe, the US and Japan. In 1927, a local telephone call in Britain was twice as expensive as in the US and three times as expensive as in Norway or Sweden. By 1915 approximately 10 million telephones were operating in the US. That latter number was only reached in Britain more than half a century later, in 1965 (Marvin 1988:64; Canes 1968:18; Robertson 1947:34; Aronson 1977:23; Perry 1977:80; Hills 1986:81, 84; Wolmer 1932:48-149; see table 4.1.2, and diagrams 4.1.2a, and 4.1.2b)[13].

Year	Number of Telephones	Related as Percentage of the Population
1890	45,000	0.12
1895	99,000	0.25
1900	210,000	0.51
1905	438,000	1.02
1910	663,000	1.48
1915	818,000	1.85

Table 4.1.2: Telephones as a percentage of the population in the UK, 1890-1915. Adapted from Perry 1977:82.

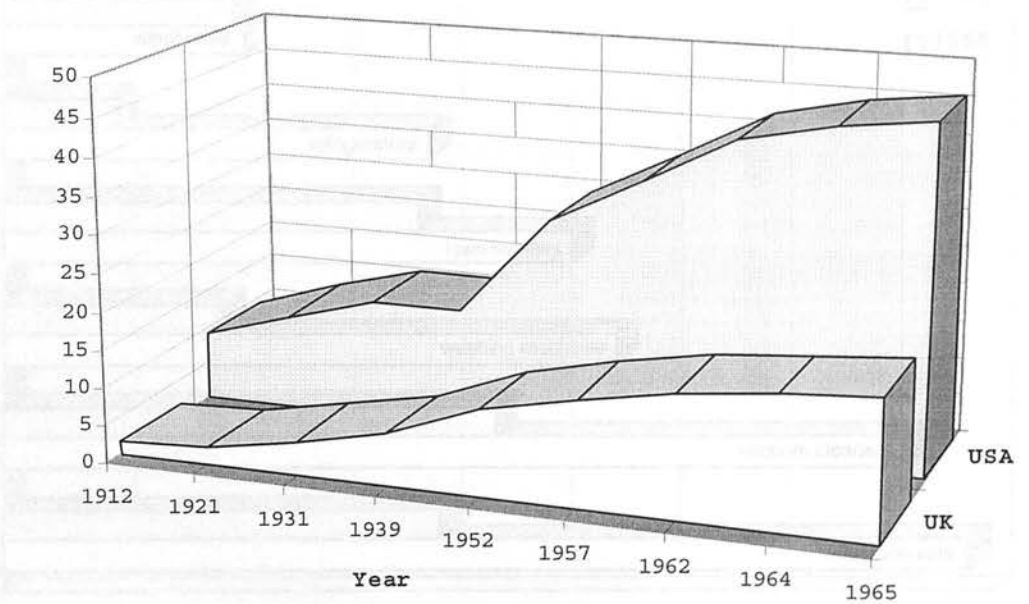


Diagram 4.1.2a: Comparison of telephone penetration in the UK and the US. Adapted from Canes 1966:18.

[12] Originally cited in the technical journal *London Lightning*, 27 June 1895, p447.

[13] International comparison is, of course, not the only method of confirming the stagnant course of telephone development in Britain. It can also be demonstrated through the comparison of the dissemination of telephones against a number of other household appliances such as, say, refrigerators, washing machines and television sets (see diagram 4.1.2c).

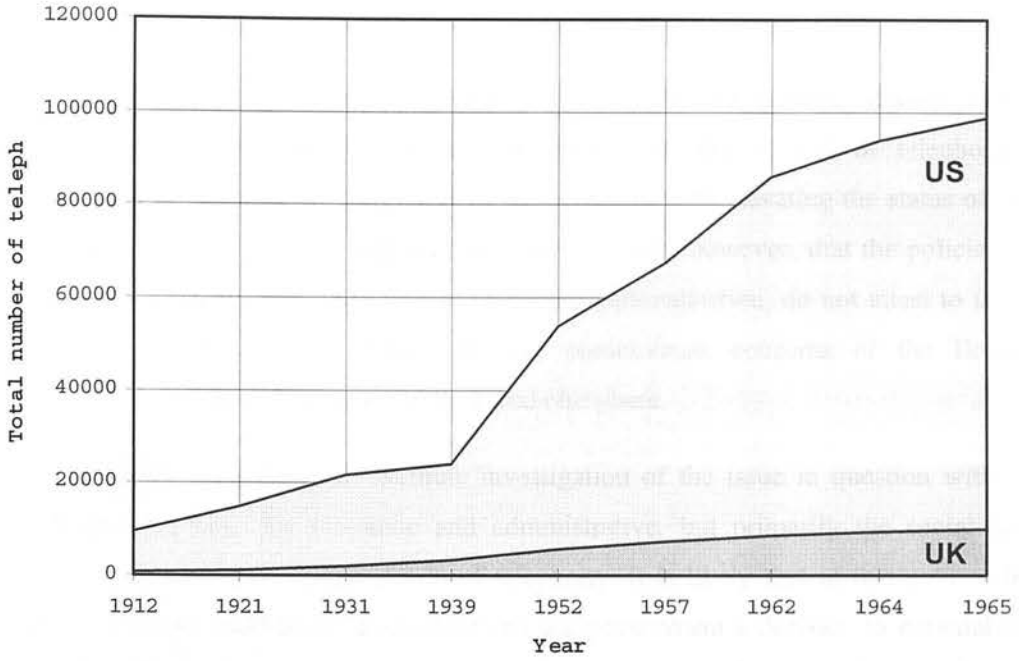


Diagram 4.1.2b: Comparison of total numbers of telephones (in millions) in the UK and the US. Adapted from Canes 1966:18.

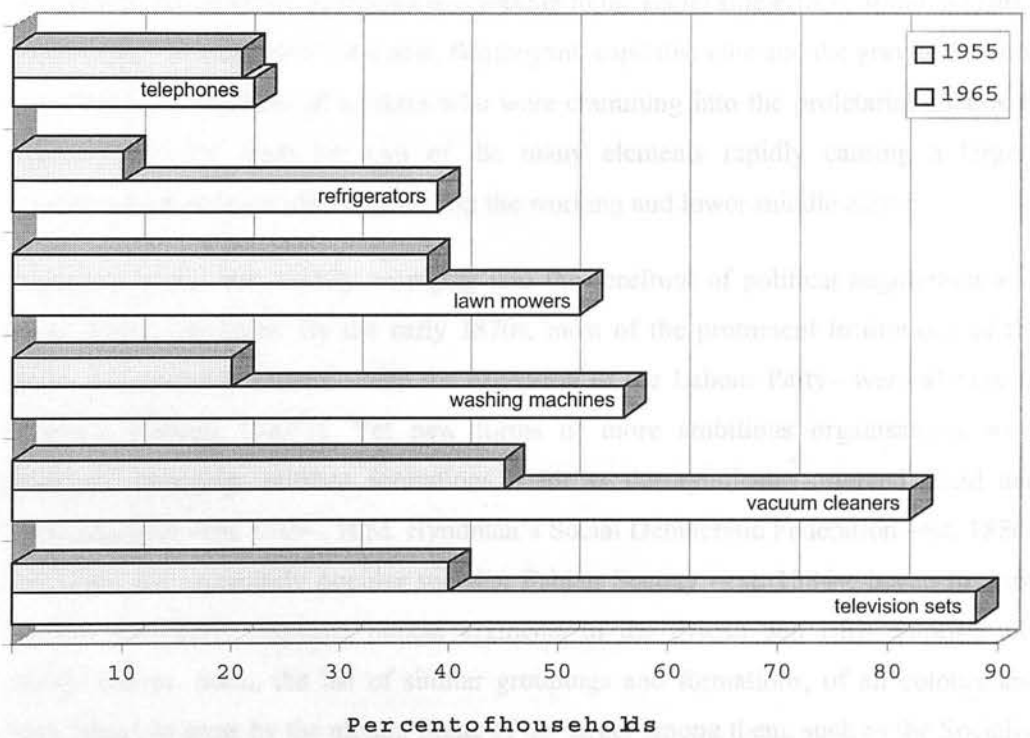


Diagram 4.1.2c: UK households owning durable goods in 1955 and 1965. Adapted from Canes 1966:24.

4.1.3. The Socio-political Context of Nationalisation.

One is not urged here to dispute that elements in successive British administrations at the turn of the century were concerned with eliminating the impact of telephony's development on the state's telegraph revenue, or indeed with elevating the status of the telephone system to that of a national asset. It is evident, however, that the policies of these administrations, both prior to and following nationalisation, do not attest to these concerns. It could well be, then, that the predominant concerns of the British government's telephony policy are to be found elsewhere.

It is impossible to conduct an accurate investigation of the issue in question without examining, not only the economic and administrative, but primarily the social and political context of the nationalisation of telephony. It is likely that in this context lie some of the more significant motives behind the government's decision to nationalise. More specifically, one needs to question the extent to which ideological factors influenced the takeover of telephony. The second half of the 19th century was a period of heightened class conflict, as Britain was waking to the social side effects of the industrial experiment. The emergence of a new, flamboyant, capitalist elite and the grave economic degeneration of millions of workers who were cramming into the proletariat ghettos of industrial centres, were but two of the many elements rapidly causing a largely unprecedented political militancy among the working and lower-middle classes.

Organised labour was rapidly emerging into the forefront of political negotiation as a major mobilising force. By the early 1870s, most of the prominent institutions of the labour movement in Britain –with the exception of the Labour Party– were already in existence (Hinton 1983:1). Yet new forms of more ambitious organisations were gradually emerging: militant formations, such as the syndicalist-oriented Land and Labour League –est. 1869–, H.M. Hyndman's Social Democratic Federation –est. 1880– and, later, the immensely popular socialist Fabian Society –est. 1884–, began to draw together previously disparate radical segments of the British and Irish working and middle classes. Soon, the list of similar groupings and formations, of all colours and sizes, began to grow by the month. Some of the larger among them, such as the Socialist League –est. 1884–, the Scottish Labour Party –est. 1888– and the Independent Labour Party –est. 1893– were behind the appearance of numerous radical publications, society

clubs and propaganda offices throughout Britain[14].

Perhaps the most remarkable feature of that phenomenon was the striking growth of trade union membership throughout the nation. The latter grew from less than 500,000 in the mid-1870s to over two million by 1899. The dawn of the new century witnessed in Britain the rise of the most extensive and organised trade union movement in the world: by 1914, trade union members accounted for more than a quarter of the total workforce, upwards of 4 million workers in virtually every British industry, with total union membership growing, on average, by 1 million per year[15] (Hinton 1983:24, 84; Wigham 1976:33; Morgan 1987:14).

Interestingly, the primary reason behind this unprecedented upsurge in union membership was not the deteriorating conditions in the workplace. In fact, working conditions had remarkably improved since the 1850s (Hunt 1981:76-98). It was, rather, the increasing administrative capacity of trade union organisations to manage, monitor and steer large numbers of members throughout the nation. In his study of British working class movements, economic historian E.H. Hunt takes after S. and B. Webb in describing late 19th and early 20th century unions as 'new model unions', distinguished from the old by their advances in union organisation, communications efficiency and technical skill (Hunt 1981:250; Kirk 1994:76).

It was this very organisational efficiency that led to the gradual formation of networks of co-ordination between geographically disparate labour organisations. Already, by 1860, networked trades councils had appeared in every sizeable town and city in the British Isles (Hunt 1981:264), while some unions, such as the Society of Engineers had set up networks of paid correspondents in all of the nation's industrial centres (Wigham 1976:2). Other unions had extended their ties to international labour bodies: Karl Marx's London-based International Working Men's Union co-ordinated and held annual congresses in 6 different European cities between 1865 and 1872[16]. Increased

[14] Political militancy ran parallel to a resurgence of nationalism. Since 1858, the first semi-secret Irish republican organisation, the Fenian Brotherhood, and thousands its of members in America, had declared war against Britain. Other militant Irish republican organisations, including *Clan na Gael*, emerged at the turn of the century in the United states, Australia and Canada, co-ordinating a campaign of sabotage and subversion directed against the British state and its interests in Ireland and the world (Porter 1987:26). The colonies were another fertile ground facilitating the growth of anti-British sentiment among the native population. Already by 1910, nationalist and other radical political networks were operating in Southeast Asia, the Middle East and sub-Saharan Africa, promoting the violent overthrow of the colonial forces.

[15] Total union membership in Britain had soared to 8 million by 1919 (Morgan 1987:14).

[16] The conferences were held in London (1865), in Geneva (1866), in Lausanne (1867), in Brussels (1868), in Berne (1869) and in The Hague (1872) –see Beer (1920:217).

networking gradually encouraged the amalgamation movement, which decisively altered the history of British labour unionism: in 1908 the Miners' Federation of Great Britain incorporated the last independent miners' unions of north-eastern England to become the first national union body. The National Transport Workers' Federation[17] followed in 1910, as did the National Union of Railwaymen (1912). Finally, in 1914, there came the Triple Alliance of miners, railway and transport workers, which

> provided for the co-ordination of strike action between its constituent unions [and] was widely seen as a portent of a revolutionary general strike movement [Hinton 1983:91-92; see also Jeffery & Hennessy 1983: 1-2].

At the end of the 20th century's first decade, Trade Unions Council (TUC) annual meetings involved the almost daily request and co-ordination of the voting preferences of more than 1,5 million union members located all over the British isles (Beer 1920:316). Through such co-ordinating procedures, the systematisation of Parliament lobbying, national walkouts, and collective bargaining lent unions "an amount of power which would surprise a modern trade unionist" (R.W. Postgate ctd in Hunt 1981:262).

This power was unleashed during large, carefully co-ordinated and national, or general, strikes – a form of organised action that "emerged as labour sought to override the constraints of locality through trade union organisation" (Charlesworth *et al.* 1996:xiii). The 1852 and 1897-1898 Amalgamated Society of Engineers national lock-outs; the nine hours movement of 1871, the field revolts of 1872-1874, and the May Days of 1890, 1891 and 1892, which involved the co-ordinated participation of more than 3 million demonstrators from Aberdeen to Plymouth (Charlesworth *et al.* 1996:112-115), brought back memories of the Chartists and the General Strike of 1842. But it was the railway strike of 1911 that truly shook Britain: it was the first ever railway strike on a national scale and the country was brought to a complete halt. The government had to react rapidly, and they placed at the service of railway company managers every British soldier in the country. The strike was not over until troops were stationed on the streets of most large towns and cities, and martial law was declared over most of the nation (Hinton 1983:86ff)[18]. A particularly frightening –for the government– phenomenon was

[17] Renamed Transport and General Workers' Union in 1920.

[18] According to Hinton (1983:86) "[t]his was no ordinary strike movement. The spontaneity and breadth of the strikes posed unprecedented problems [...] for the forces of the state [...]. And the longer settlements were delayed the more the strikes took on the character of a general social war [...]. Troops were called out in several centres, and Salford was subjected to virtual military occupation. In Liverpool, with a gun boat standing by on the Mersey, two strikers were shot dead by the Army following three days of guerrilla warfare in the streets around the city centre".

that of sympathy strikes. In these, networked union groups around the country would walk out in support of a local labour dispute, even if the latter concerned a completely unrelated part of the industry hundreds of miles away.

> No community could exist if resort to the sympathetic strike became a general policy of trade unionism [ctd in Wigham 1976:29],

wrote Sir George Askwith, a senior Labour Department civil servant, at the time. A few months later came the most dramatic labour dispute on a national scale until the 1926 General Strike –"the biggest stoppage the world had yet seen" (J. Lovell ctd in Kirk 1994:107): less than four years after its national amalgamation, the Miners' Federation of Great Britain called out a national strike on March 1, 1912. It was the first national miners' strike ever and found the nation totally unprepared. Within days, 600 factories had closed down due to lack of energy, while all rail services were stopped and 1 million workers had been laid off. Soon, coal prices had reached famine levels (Hinton 1983:85). Throughout the strike, the British press, as well as the public and many politicians were under the impression that a revolution, or total breakdown of society, was imminent. Sir Edward Gray, MP, characteristically wrote to a friend:

> [t]his coal strike is the beginning of a revolution. Power has passed from the King to the nobles, from the nobles to the middle classes and through them to the House of Commons and now it is passing from the House of Commons to the trade unions [...]. The unions may of course, like blind Samson with his arms round the pillars, pull down the house on themselves and everyone else, if they push things too far; or if the owners are unyielding, there will be civil war [...]. There are unpleasant years before us [ctd in Wigham 1976:28].

The above quote is indeed typical of the times. It signifies the realisation among governing circles that union groups had amassed organisational skill, networking power and large numbers of members who were now "capable of national strike action that could bring the whole economy to a halt" (Hinton 1983:93). By means of this realisation, the British state –represented by the Department of Labour and the Cabinet, which until then had adopted a policy of non-involvement with industrial disputes– began to proceed to what Jeffery & Henneseey (1983:3ff) have described as "the creation of an official strikebreaking machine". This security machine was exposed in 1919 –following yet another paralysing railway strike– in a report produced by the General Headquarters Great Britain[19] and submitted to the War Office (ibid:22ff). The largest part of the report

[19] The Headquarters was established shortly before the Great War with the aim of conducting military operations at home.

concerns the communications between troops and other emergency services, and makes particular mention of telephones as valuable instruments for combating strikes. There is also a request that, in their efforts to control union strike activity, officers "should have the right to use public call telephones without payment", since the latter belonged to, and were used for the interest of, the government (ibid:22).

Arguably, the technical means of facilitating the increasing national co-ordination of union activity must have had largely to do with the telegraph and, later, the telephone. Instantaneous communications would have been the only means by which synchronised, collective action involving the simultaneous involvement of millions of union members, separated in local associations throughout the British Isles, would have been realistic or indeed possible. The dramatic potential for "reorganisation of the social geography" (Marvin 1988:66) offered by the new, instant communications systems was probably used to augment the coherence, timing and efficiency of labour struggles. At the same time, it would seem equally plausible that the government would be interested in employing the instant communications network for the purpose of co-ordinating its response to such all-encompassing subversive activities –as illustrated by the aforementioned 1919 report to the War Office.

Unfortunately, the relevant research literatures[20] contain virtually no consideration of the nationalisation of telephony in the context of the rapid radicalisation of British society during the late 19th and early 20th centuries, or indeed in the context of the increasing governmental intervention in industrial disputes. Instead, most of the literature on the nationalisation of telephony views the latter incident as a fundamentally financial decision –an extension of the nationalisation of telegraphy. Yet, if we were to infer by reference to telegraphy, we would have to consider a number of very real non-financial factors that might have influenced the decision to nationalise cable communications. The telegraphy nationalisation debate, which took place in the late 1850s and early 1860s[21], was indeed mirrored by the telephony nationalisation debate, which followed a few years later. Public frustration mounted over the high dispatch fees charged by private-owned telegraph companies, which limited its use to a small, wealthy elite (Kieve 1973:126).

[20] Including works on trade union history and organisation, social aspects of the telephone and governmental attitudes to telephony.

[21] According to Perry (1992:91) "[b]y 1861 the major arguments for nationalisation (a lower as well as uniform scale of tariffs, greater economies of scale, the successful operation of continental state-owned systems, and the importance of vital communications being in public hands) had all been clearly enunciated".

There was a class of civil servants who viewed a possible nationalisation as the state's duty to provide a social service, spreading telegraphy to rural areas and uniting the nation through the immediacy of telegraphic contact (Perry 1992:89, 111, 119). Finally, there existed amongst legislators the belief that telegraphy was too significant an asset to be abandoned at the hands of profit-oriented corporations:

> [i]t seems to me, indeed [...] that the transmission of news [...] throughout the Kingdom should be regarded as a matter of national importance and that charge for such transmission should include no greater margin of profit than to suffice to make the service fairly self-supporting [F.I. Scudamore, Accountant General of the Post Office, ctd in Perry 1992: 105; see also Kieve 1973:146].

Yet, the research literature also reveals a debate running in parallel with the more widely-distributed discussions on financial inclusion and social service provision, namely the debate on the political significance of the state's control of the communications networks. It is often ignored that, before the first Telegraph Act of 1854 was even debated in Parliament, telegraphy had already been nationalised in a number of British colonies, including India. It was there that the British government was able to explore the military control, communication and command uses of the new technology. James Dalhousie, who had been instrumental in the nationalisation of telegraphy in India as the London-based Governor General of the East India company, viewed the technology not as a business venture, but as an instrument of British military might –a device which had contributed to "the early realisation of a vast magnitude of increased political influence in the East" (Dalhousie ctd in Headrick 1991:52). In 1854, soon after the proposal for the nationalisation of telegraphy in India was enacted, he wrote a friend:

> [t]he post takes ten days between [Calcutta and Bombay]. Thus in less than one day the government made communications which, before the telegraph was, would have occupied a whole *month* –what a political reinforcement this is! [ctd in Headrick 1991:52].

In 1857, the rulers of the Empire had the opportunity to decisively test the telegraph in action during the large Indian army mutiny, which engulfed most of northern India and was the strongest challenge to the British Empire since 1776. The outnumbered and outgunned British forces used the new communications instrument to surround and capture the mutineers. Following the crush of the rebellion, Commissioner for the Punjab, John Lawrence, is quoted as having declared that "[t]he telegraph saved India" (ibid.:52). Headrick (1991) informs us that, following the subversion of the Indian

rebellion, the telegraph spread in all areas of the British Empire largely due to "the military and political needs of the British rulers" (ibid.). Africa was one of those areas. In 1877, Thomas Watson, president of the Cape Town Chamber of Commerce, wrote to the Cape's governor arguing in favour of the establishment of telegraphic communications with London:

> [t]he construction of a line of telegraph through the centre of this great country would not only put us in immediate communication with the mother country, but at the same time open up a vast field for commercial enterprise. The maintenance of a series of stations along the route would do more to abolish the slave trade than [...] a fleet of cruisers on the African coast. Mission stations would be protected, savage tribes civilised and in a few years a complete revolution would be effected [ctd in Headrick 1991:62-63].

Requirements relating to the co-ordination and defence of the Empire at large, at that time more geographically stretched than ever before, were also thought to be fulfilled[22] through the use of electric telecommunication systems. According to Irish historian and philosopher W.E.H. Lecky, the use of the telegraph had "at least modified the Irish difficulty by bringing Dublin within a few minutes' communication of London" (ctd in Marvin 1988:98). Celebrating the initiation of the operation of an 8,100-mile telegraphic circuit connection from New York to London in 1880, the British Special Commissioner to Canada, Henry Norman, characteristically stated:

> [i]s not the click of this key (heard in two hemispheres) more eloquent than all the arguments of empire ever penned? [ctd in Marvin 1988:98].

Such beliefs were successfully transferred to the mother country during the telegraphy nationalisation debate. Marvin (1988:98) agrees it was not long after the appearance of electric communication that the British state recognised its significance for political assertion and social control. It was often presented as "a superior means for controlling masses, criminals, primitives, servants, and whatever other underclasses might need restraint" (ibid.:100). According to the *London Electrician*, riots and other 'unruly meetings' that took place every winter in West London could be countered by the empowerment of electric communication, demonstrated by its ability to collect and co-ordinate a large police force "at any desired point, within a very short time" (7 July

[22] It is not my intention to claim that such hopes were indeed materialised. It should be remembered that the British Empire crumbled after its rulers had established total telegraphic and telephonic interconnectivity between the main strategic centres within its borders.

1888, ctd in Marvin 1988:99). Lecky wrote in 1896 that electric communications had "greatly strengthened the central government in repressing insurrections, protecting property, and punishing crime" (ctd ibid.).

In 1861, legislators J.L. Ricardo and W. Burchell produced a report in which they accused the private telegraphy companies of being "individual and irresponsible" (Perry 1992:90), while asserting that publicly-elected statesmen should be in charge of enhancing the system's military and diplomatic usefulness (ibid.). Others contributing to the debate directed attention to the usefulness of the electric telegraph as a means of communicating and acquiring intelligence (Kieve 1973:124). It was precisely for this reason that many concerned actors and observers positioned themselves against the nationalisation of the telegraph. The danger of government espionage against its citizens "as practised in Europe" was one of the private telegraphy industry's primary arguments against nationalisation (EITC 1868:12-13). The national and local press repeatedly raised the issue (Kieve 1973:145) and a House committee was set up to investigate "what securities should be taken for insuring the secrecy of messages transmitted through the Post Office" (ctd in Kieve 1973:148). A member of the committee, George Leeman, MP, raised the issue of state agencies potentially intercepting telegraphic communications between subscribers by reminding Parliament of the notorious scandal of the interception of Joseph Mazzini's[23] mail correspondence by the police, a few years earlier (Perry 1992:108).

The parallel between postal correspondence and telegraphic communication is indeed quite appropriate. Kieve (1973:124) has indicated that, throughout the debate on telegraphy nationalisation

> [i]t was argued that many of the reasons for the Post Office being made a government department seemed equally applicable to the telegraph [Kieve 1973:124].

Kieve does not particularly substantiate this claim with extracts from the broader debate. Yet, providing his claim is indeed accurate, it is a crucial step in determining a security and policing element in the communications nationalisation debate. Scholars are in

[23] This was the first ever public controversy over state-sponsored communications interception in Britain. It occurred in 1844, when it surfaced in the English press that the Home Secretary had issued a warrant for the interception of the correspondence of the Italian revolutionary Joseph Mazzini, who resided in London (Baxter 1990:161).

agreement that the 1657 Ordinance Act, which was enacted during the Cromwellian period and which established the government's postal monopoly, was primarily a security measure aiming to enhance the government's control over the content of postal correspondence. The Ordinance Act itself describes the monopoly as "the best means to discover and prevent any dangerous and wicked designs against the Commonwealth" (Bunyan 1976:197; Baxter 1990:160-161; Fitzgerald & Leopold 1987:36). According to Sir Edward Murray, former General Secretary to the Post Office,

> [t]he original object of the state monopoly was not so much to extinguish competition as to give the government of the time access to the correspondence of suspected persons, and particularly to letters passing between England and foreign parts [Murray 1927:3].

Undoubtedly, this significant political element of governmental control of communications, which was present in the postal and telegraphy monopoly debate, was also present in the controversial discussions around the nationalisation of telephony. Its absence from the existing literature is not an assurance of its non-existence; rather it is a manifestation of the way in which economic-oriented deterministic accounts of the nationalisation process have been favoured in the expense of a more holistic approach, incorporating the role of social, political and ideological elements in the process.

There are, of course, many more crucial issues that remain unresolved: how does, for instance, the nationalisation of telephony relate to the expansion of the social regulatory role of the British state during the first decades of the 20th century, and especially the co-ordination of the extended suffrage after 1906 (Pugh 1978:29-44)? How are we to explain the nationalisation of telephony in light of the gradual creation of a war economy in Britain, prior to the outbreak of the Great War –a development which also signalled the government takeover of wireless broadcasting under the Defence of the Realm Act (DORA) (Headrick 1991:145; Briggs 1961:20)? Equally importantly, what was the position of the British military –a particularly vocal actor in all aspects of communications regulation (Hughes 1981:35ff)– in the overall debate on nationalisation? Finally, how did the moral question behind the explosion of gambling and prostitution, two industries which made frequent use of the telegraph and the telephone to organise their business and attract customers, influence the debate on

telephony nationalisation[24]?

None of the above questions are even acknowledged in the relevant literature. Yet it was in this very social context, at this period of rapid social and political change at all levels, that the nationalisation of telephony was implemented. The fear of a potential loss of social control over the organised, underprivileged manual workers[25], as well as the latter's apparent rejection of bourgeois common sense, social norms and morals, the threat against British global superiority in an increasingly competitive international market, as well as the mounting resentment by Irish and other colonised peoples against British rule, were all partial ingredients in an explosive mixture of threatening socio-political insecurity that was dominating British elite sentiment. This deep feeling of insecurity was anything but pacified by the arrival of the telephone. The telephone network proclaimed a radically different mode of social and political negotiation, an inter-connectivity that could be used to connect and mobilise critical masses of dissidents who were previously scattered along the four corners of the nation. It also represented a dramatic "reorganisation of social geography" (Marvin 1988:66), which had the potential, if used in certain ways, to augment the coherence and efficiency of political protest, as well as all sorts of indecent venturing.

An examination of the take-over of telephony through the prism of the social context expressed above, would have an enlightening effect on contemporary understanding of the British government's decision to nationalise voice telecommunications. The decision

[24] Prostitution and gambling were virtually revolutionised with the adoption of the telephone. By the late 1880s no self-respecting brothel lacked one or more telephone instruments through which customers made their reservations. The immense impact of the new communications medium on prostitution –at the time of the emergence of the telephone, approximately 50,000 prostitutes were operating in the greater London area (Thompson 1968:59)– can also be observed in the emergence of a new term: the more traditional words 'harlot' or 'prostitute', were replaced by the expression 'call girl' (Pool *et al.*1977:136). Gambling, already forbidden by law from advertising in most print publications, switched to the adoption of the telephone as its foremost operating medium (Petrow 1994:259; see also Munting 1996:27). In fact, it was often the case that such ventures were stationed abroad, outside the rule of British law enforcement. The use of the telephone network by gamblers and call girls became so extensive that, at the turn of the century, the very influential at the time National Anti-Gambling League, along with numerous other anti-gambling and anti-prostitution organisations, accused the National Telephone Company of knowingly acting as 'commission agents' and 'messengers' of illegal and indecent operations stationed in Britain and abroad (Pool *et al.* 1977:136; Petrow 1994:265). This moral frustration generated one of the most tension-ridden single-issue campaigns of the times –one that can be in many ways compared to the American alcohol prohibition movement, which followed a few decades later (Petrow 1994:250ff).

[25] According to Morgan (1987:14), such developments inspired "a mixture of respect qualified by fear".

sought to promote and safeguard the interest of the nation, as was indeed often argued at the time (Robertson 1947:45), though not just in economic or administrative, but perhaps also in social and political terms. Apart from technical data and revenue statistics, political convictions and ideologies, as well as competing visions of the 'national interest', were undoubtedly instrumental in the decision to nationalise.

4.2.0. US: Regulating Deregulation.

It has been documented that, in the US, the 15 years following the establishment of the Bell Telephone Company in 1876 were characterised by ruthless competition between inventors, capitalists and investors, and marked by the absence of governmental regulation (Cohen 1992:22). Striking indeed during those years was the frequency by which Bell was called upon to testify in lawsuits brought by individuals claiming to have invented the telephone before him[26]. It would be reasonable to assert that the early assumption of the Bell Telephone Company's monopoly control over the telephone market was a direct result of the inventor's ability to soundly affirm the legal validity of his patents (ibid.:23, 24).

The relaxed posture of the American government during those early years should not be interpreted as an indication of passivity. It would, of course, be erratic to attempt to distinguish a unique and monolithic motivational element behind governmental activity in the area, especially since the latter was expressed as a series of rapidly shifting positions and policies throughout the late 19th and early 20th centuries. The following example is illustrative of this: in 1895, Bell's monopoly patents expired, leading to a decade of fierce competition among rival telephone companies. Being by far the most powerful among these, the American Telephone and Telegraph (AT&T) initiated a voracious wave of successive takeovers aiming toward the establishment of a nationwide telecommunications network. It was in 1913, therefore, when the US government brought forward a federal anti-trust lawsuit against the company. Yet shortly afterwards, while in the process of negotiating an out-of-court settlement, the government arrived to the conclusion that the specific nature of the telephone enterprise meant that the public interest would be favoured by the economic integration of the system. Consequently, as

[26] The long list included, apart from Elisha Gray, the American inventor Thomas Edison. Although several suits reached the US Supreme Court, the latter upheld Bell's rights in all cases.

it is often put by historians, an AT&T monopoly was "not discouraged" by government (Canes 1966:12).

The decision of the government to allow AT&T to develop in a protective, monopolistic environment permitted the company to assume and retain centralised control of what was to rapidly become a most profitable market. In return, the state reinforced its regulatory role as the *ad hoc* guarantor of the development of an essentially private, capitalistic undertaking (Garnet 1985:3; Temin & Galambos 1988:12). In this manner, the government was in a position to oversee and press not only for the successful application of the telephone system onto the life of the nation, but also for the development, compatibility and overall co-ordination of an enterprise that was seen to be an important national asset.

It is a truism that the very history of telephony in the US is a case study on the structural centrality of state institutions in a deregulated environment (Teske 1990:17ff). As early as 1907, a series of states began to form public utility commissions, that is, regulatory bodies responsible for countering possible pricing and other market abuses by monopolistic enterprises, including AT&T. By 1913, public utility commissions were overseeing the AT&T's operations in no fewer than 34 states, with at least a dozen more considering the formation of similar public regulatory bodies (Garnet 1985:130ff, 191; Teske 1990:2). In 1934 the Interstate Commerce Commission (ICC) was succeeded by the Federal Communications Commission (FCC) as telephony's primary federal regulatory body. Soon afterwards, AT&T was reaching its target of owning approximately 80 per cent of the country's telephones[27], thus becoming virtually synonymous with the national telephone network (Teske 1990:2). Yet, the acceleration of AT&T's oligopoly was accompanied by a parallel acceleration of the state's regulatory power. The contradictory relationship between capitalist competition and monopolisation was expressed in a series of successive antitrust suits brought against the company by the FCC and by other governmental institutions. Wishing to keep AT&T on a state of constant alert and caution, the government often encouraged debates centred on nationalisation within its circles (Cohen 1992:23), so much so that a contemporary observer remarked:

[27] A share that was retained until 1982 (Teske 1990:2).

> [w]hether the US shall continue a democracy, or shall revert to a form of oligarchic control, imposed by corporate states through assumption of state powers, today hangs in the balance [Danelian 1939:380].

After World War II, AT&T continued to function and prosper under the, mostly protective but often restrictive and penalising, shadow of the state apparatus. Contradictory decisions by government, as well as decisive policy splits within its ranks, were based on the skilful balancing of a variety of principles, such as the public utilisation of telephony, control over a powerful communications medium, market competitiveness and national security. The overall co-operation between the state and AT&T was the outcome of constant negotiation between them, as well as their will to embrace economic, cultural and political targets that satisfied both[28]:

> [t]his has not always been easy or possible, and has often led to conflict between the government and AT&T. However, it is in the interests of both parties to find a mutually acceptable position because of the impact of both actors on each other and their desire for amicable relations [Cohen 1992:20].

4.2.1. Telephony and the National Interest.

The adoption of mutual targets by the institutions of state and telephony are epitomised in their functional co-ordination in pursuit of the national interest[29]. The close political relationship between successive American governments and telephone companies is widely known and has been extensively illustrated by diplomatic historians and other researchers. According to Martin (1991:46), "strategic political connections" between the Bell Telephone Company and the US government began forming as early as 1877, before the company's incorporation. The "unique relationships" (Temin & Galambos 1988:9) between the company and state, as well as federal, policy centres in all levels created a "peculiar framework" (Aronson 1977:7) of intimate institutional relations, under which managers of AT&T, International Telephone and Telegraph (IT&T) and other telephone companies operated for many decades.

The efficacy of that institutional framework was strengthened, not only by the presence

[28] One such mutual target was the aspiration that the telephone system in the US should become a universal and affordable service. The complexities of this decision, which constitutes a direct opposite of British policy on the subject, have been extensively illustrated in Pool *et al.* 1977:130ff; Aronson 1977:27ff; Temin & Galambos 1988:6, 11, 15-16, 20; Martin 1991:26ff, 107; as well as in Cohen 1992:5, 30, 49 and Teske 1990:130.

[29] A set of policies, that is, which produce and maintain a dynamic arrangement of national and international parameters favouring the successful exercise of the nation's military, political and economic domination.

of powerful political allies in Congress (Temin & Galambos 1988:25), nor simply by the numerous political lobbyists operating in Washington DC (Sampson 1973:183ff)[30], but also by the frequent exchange of technical and administrative staff between government agencies and the companies. During World War II, for instance, the Pentagon was employing considerable numbers of former, as well as future, IT&T employees (ibid.:38). According to Sampson (1973:183), there have always been extraordinary numbers of former Pentagon officers within the ranks of IT&T staff: "in 1968 they included three rear-admirals, two brigadier-generals, 22 colonels and eight captains". What is more, during the 1970s, the IT&T executive board included J. McCone, former Director of the CIA (ibid.:99).

Upon the end of World War II, Paul Porter, Chairman of the FCC, made the following strategic remark:

> [today,] the managements of international communications companies are in a position to shape our international communications policy through their ability to negotiate and make arrangements with the representatives of foreign governments [1945, ctd in Sampson 1973:22].

The case of IT&T is particularly illustrative of this issue. The company, undoubtedly one of the largest in the world, with offices in more than 140 countries around the globe, was actively involved in the defensive and offensive plans of the US government during the Cold War (ibid.:56). Prior to the nationalisation of IT&T's ventures in the, then newly founded, communist republics, the CIA had placed agents in the company's offices throughout the Eastern Block, under the full knowledge and approval of S. Behn, the corporation's founder and –at that time– president. More agents were placed in Latin American nations including Bolivia, Paraguay and Argentina (ibid.:41). It would not be inappropriate to claim that, in at least two instances during the Cold War, in Hungary and Chile, IT&T *made* American policy as much as it followed it (ibid.:269).

After the end of World War II, in anticipation of an imminent third world war fought between capitalist and communist countries, and in an attempt to act in defence of American interests, Behn secretly ordered the corporation's managers in Budapest to slow down and even sabotage production in every possible way. His decision was made

[30] D. Beard, IT&T's formal political lobbyist at the US Congress during the 1960s, once characteristically remarked that "you need to know what is going on in Washington, or you can't run a company" (Sampson 1973:183).

"with the understanding of the US General Staff" (ctd ibid.:51). In 1949, Budapest-stationed IT&T Eastern Europe Area Manager Robert Vogeler was arrested by the Hungarian military police on charges of practising intelligence espionage on behalf of the US. During the four-day trial that led to his execution, Vogeler explained in his own words that

> the co-operation between the [Hungarian branch of IT&T] company and the [US] military was such that the latter could control the operations of the company [ctd in Sampson 1973:50, 53].

A little more than two decades later, on March 21 and 22, 1972, *Washington Post* journalist Jack Anderson revealed that leaked IT&T documents showed that the corporation had, two years earlier, plotted with the CIA and elements in the US government to block the election of Salvador Allende, Chile's left-wing president. Fearing a possible nationalisation of its ventures in an Allende-governed Chile and in a potentially Marxist-dominated Latin America, the company had tried to sabotage production and help encourage a military coup. It had also offered a series of six-figure sums to the White House and the Republican Party. In return, the government dropped a series of antitrust lawsuits against IT&T (Bertrand Russell Peace Foundation 1972:4, 238; Sampson 1973:232).

There was no statement by the CIA regarding the disclosure. However, IT&T executive board member and former Director of the CIA J. McCone admitted that IT&T executive personnel and representatives of the US government had indeed discussed –though not acted upon, he said– plans to undermine Allende's candidacy (Sampson 1973:238).

4.2.2. Regulatory Discretion as a Platform of Negotiation

In the US, the decisions of successive government administrations not to nationalise telephony appear to have been in harmony with the predominant free-market doctrines of the time. The appearance of telephony was interpreted more as a supplement to telegraphy and less as a threat to it. Additionally, the absence of any systematic revenue-oriented state intervention in telegraphy allowed the government to adopt a discreet role among concerned actors, while encouraging private entrepreneurs to take investment initiative and spread the use of the telephone throughout urban centres.

Yet it would be erroneous to assume that the state's regulatory discretion symbolised its

lack of interest in the political and social uses of the new invention. The belief that telephony was a natural monopoly[31], which generated AT&T's private monopoly, was – among other things– a platform of structural interdependence and policy negotiation. It was through this platform that successive US administrations were able to effectively promote the incorporation of the state's political, diplomatic and security concerns into the broader spectrum of AT&T's market ambitions. Gradually, the very same platform was used by the corporation and by its international subsidiary, IT&T, to promote US diplomatic agendas that were in agreement with their own market-based executive decisions.

4.3.0. Summary: Regulation as a Political Choice.

In both the UK and the US, the early history of telephony was marked by constant negotiation between concerned actors attempting to define the usefulness of telephony, as well as its role in society. The debate was characterised by a spectacular array of changing policies and shifting positions, as well as by the intervention of governmental institutions, technicians, politicians and business conglomerates. The social and economic priorities of governments in Britain and America have varied tremendously. In Britain, the principles of open market and free competition, upon which the country's economy had been built, were sacrificed in favour of the national interest and, perhaps, social harmonisation. In the US, the fragile equilibrium of economic competition and state supervision was pursued in an attempt to ensure widespread access to the telephone.

In both cases, however, the role of the state in shaping and defining the features of the new technology has been overwhelming. It manifested itself through diverse policies: in Britain through the complete and incontestable takeover of the industry by the Post Office and in America by rigid and constant regulatory surveillance by the federal government as well as by individual state administrations. Though distinct, both sets of policies display a common unifying element: they were formed and operated in conjunction with the traditional characteristics and functions of the state as a historical force. Their goals, far from the pursuit of abstract notions of right and wrong, was

[31] Natural monopolies are created when the financial, social and geopolitical features of national or other territorial economies are such that to have more than a single company operating in a specific market would be detrimental to the consumer body as a whole.

"deduced from history and enacted into law" (Pierce 1977:193). Ultimately, no nationwide communications network could be implemented without the political approval and close administrative supervision of the executive vanguard of the nation.

It has been claimed that, due to its technical features, no industry renders itself more readily applicable to state management than telephony (Mavor 1916:2-3). Similar to other public utilities, such as gas, electricity and water distribution networks, the argument goes, the telephone service is a "natural monopoly" (Pierce 1977:192). Yet, that argument dangerously excludes the complexities of monopolistic regulation by reducing the latter to a matter of technical necessity. The fundamental nature of the state's involvement in telecommunications is not only technical, but also social and political (Canes 1966:12-3). Fundamentally, in Britain and America, state regulation over telephony was dominated "by changing ideology, not changing technology" (Temin & Galambos 1988:7-8).

Chapter Five

The Interception of Communications in Historical Context

5.0.0. Introduction.

In attempting to elaborate upon the particular features of the intricate relationship between telecommunications and law enforcement, a vital dichotomy may be of assistance; namely that between the communications of policing and the policing of communications. The former signifies the uses of telecommunications by law enforcement bodies for the functional and administrative enhancement of their organisation, while the latter involves the expansion of law enforcement's mission from the social realm to the realm of electric –and, eventually, electronic– communications.

The present chapter is structured in accordance to the aforementioned dichotomy. The first section, therefore, examines the early attitudes of law enforcement agencies concerning telephony, and follows these attitudes as they developed over time, in an attempt to explore the initial crucial interactions between policing apparatuses and voice telecommunications in the UK and the US. The second section engages in a discussion of British and American historical experiences of government-sponsored CI, from the time of the emergence of telephony until the end of the Cold War. The focus here is on exploring the phenomenon of CI as an element in the institutional relationship between law enforcement agencies and the telecommunications industry –a relationship that has been significant in facilitating and shaping institutional practices of CI for the largest part of the 20th century.

5.1.0. Britain: Bobbies on the Line.

In the British Isles, the police appeared as the local version of a Continental concept that emerged from the ashes of the French Revolution of 1786. Historians essentially regard it as a two-headed creature, established, on the one hand, to protect commercial and state interests from the underprivileged (Smith 1985:23) while, on the other hand, to assist in the implementation of citizen, electoral and welfare rights for British subjects (Talylor 1997:33).

The first organised police force in the British mainland[1] appeared in the streets of London in 1829 (Leonard 1964:3; Smith 1985:23). Following plans of the ruling Whigs to introduce a national system of policing (Philips & Storch 1994:80; Taylor 1997:23), law enforcement departments were gradually introduced in other cities, as well as in the countryside. The CID (1842) and the MI5 (1909), as well as the Special Branch (1917) were later established for the purpose of criminal and political surveillance (Verrier 1983:26, Fitzgerald & Leopold 1987:37-38).

Historians tend to differ on the degree to which British police forces throughout the country were keen on the adoption of electric communication. Some indicate that Scotland Yard was telegraphically connected to the various district police stations in London as early as 1849, less than five years after the invention of the telegraph (Diffie & Landau 1998:117-118; Leonard 1938:1). Others stress that, where electric communication and other technological appliances were successfully adopted, their adoption was usually the result of inspiring individual chief constables (Whitaker 1964:ch2). Elsewhere it is asserted that, even where "the will to mechanise" was present, it was usually hampered by lack of financial resources (Emsley 1996:75, 150). Finally, some propose that the overall situation points to the snail's pace at which technological modifications in the organisation of police work took place, irrespectively of whether individual forces and officers were in support of such changes (Weinberger 1995:37).

There is considerable evidence to support the latter proposition: from the turn of the century and even after World War I, many chief constables and the Home Secretary himself often expressed opinions against the adoption by the police of new mechanical devices, including telephones (Weinberger 1995:37; Emsley 1996:149). Consequently,

[1] The Royal Irish Constabulary had been founded in 1814.

in a number of large industrial cities, such as Liverpool, police forces resisted the installation and use of telephones until 1908 (Weinberger 1995:37n). Even as late as 1933, "nearly 200 police stations and about half of the 5,000 police houses were not on the telephone at all" (ibid.).

There is indeed little or no reason to believe that law enforcement institutions were more willing to adopt telephone apparatuses than any other inflexible, bureaucratic institution ever was. Yet, there are numerous reasons to accept that, for all its technophobia and institutional stiffness, the British police was much ahead of other state agencies in the application and use of electric communications systems. It is certainly impressive, for instance, the fact that, by 1867, all principal and sub-divisional stations in the country were interconnected through the police's private telegraph network (Smith 1985:41). Additionally, it ought to be observed, that the foremost argument against the adoption and use of telephonic communications by British police, was not a *per se* denial of the ability of the instrument to facilitate the instant co-ordination of departments nationwide, but that such function was already facilitated by the telegraph. It was for this very reason that police departments in many smaller towns and cities, which had not developed extensive telegraph systems, installed and used telephones almost as soon as the service became available (Leonard 1938:9). Certainly, by 1933, a private telephone system connected all divisions, subdivisions and police stations throughout Britain, from the Chief of Police to the last officer on the beat, through a system of call boxes scattered along the beat routes of police officers in every city, town and village in Britain (Leonard 1939:408; Walker 1997:257; Rubinstein 1973:16; Weinberger 1995:36; Emsley 1996:149ff).

5.1.1. US: Telephones and Alcohol.

In the US, the police, as a social concept and institution, were modelled after the British system (Caiden 1977:22; Diffie & Landau 1998:9). In populous New England cities, such as Philadelphia, PA, Boston, MA, and New York, NY, police forces were established between 1834 and 1838. Yet officers did not wear uniforms and functioned more like traditional community watchmen, rather than members of an institutionalised law enforcement agency. It was during the Civil War that internal political and social unrest led police forces throughout the US to aspire to a more militaristic organisational model (Caiden 1977:22; Fuld 1909:ch1). Following the Civil War, police departments

were established all over the country as semi-autonomous law enforcement bodies (Leonard 1964:18). During the years leading to the 20th century, the growth of the anarchist movement, as well as the emergence of the organised labour movement, brought about the appearance of political surveillance agencies in urban and some rural areas (Donner 1980:32). The FBI was established in 1908, while its Intelligence Division began operating in 1919[2].

Rather expectedly, the immensity of the American landscape was one of the factors that promoted the relatively swift adoption of telephonic communication by the country's law enforcement agencies. Having already adopted the use of dial telegraphs[3] as early as 1858, and of *Wirephoto*[4] soon after 1900, US police departments joined some of the earliest groups of telephone users (Marvin 1988:97; Leonard 1938:2; Pool *et al.* 1977: 138). By 1878, less than a year after the establishment of the first private telephone company, numerous police departments in Boston, MA, Washington, DC, and New York City, NY, had been multiply connected to the network. In that same year, the Chicago, IL, and, a little later, the Baltimore, MD, police departments, established a network of 170 telephone boxes scattered throughout their cities for the use of police officers on the beat (Marvin 1988:97; Leonard 1938:9; Diffie & Landau 1998:117-118; Pool *et al.* 1977:138). According to Leonard (1938:11), the success of police telephone boxes in Chicago "was so rapid that by 1893 no fewer than 1,000 street stations had been installed all over the city".

There was considerable resistance within police circles to the adoption and use of telephony in law enforcement operations (Leonard 1938:6-7, 80). Very often, elements within the state and federal police administrations were prepared to disregard their scepticism only after advantages promised by the proponents of the new technology had been aptly demonstrated (Pool *et al.* 1977:137-138). Undoubtedly, the opportunity for demonstration was offered by the wave of strikes that swept the nation in 1892, including the violent railway workers' strike in Buffalo, NY, where combined police and

[2] The FBI's Intelligence Division targeted primarily anarchist, communist and other non-mainstream organisations (Kessler 1993:65). Its functions and size were significantly upgraded with the enactment of the 1940 Smith Act, which criminalised the act of advocating the forcible overthrow of the Federal government, as well as holding membership in organised groups promoting such ideas (Evans 1972:48). "Thus the stage was set for expansion of the FBI from less than 1,000 special agents in 1939 to more than 5,000 by the end of W[orld] W[ar] II" (Evans 1972:48).

[3] The dial telegraph was an electric communication apparatus, which enabled individuals not knowing the Morse code to send messages over the wires.

[4] *Wirephoto* was an early method for the electrical transmission of images.

military operations played a crucial role in neutralising organised protests. The *Electrical Review* later remarked that the "newly established telephone apparatuses [were] invaluable aids" in recalling law enforcement and military officers from their residences (ctd in Marvin 1988:99).

Assertions that the telephone service was an invaluable tool for social control (Martin 1991:145), and that it gave law enforcement agencies a significant advantage over organised crime (Pool *et al.* 1977:137), were often propounded by police and public officials. These exclamations came to be backed by the experience of the Prohibition of liquor, as well as of illegal gambling operations, during the ten years following 1913[5]:

> [as] Prohibition coincided with the telephone system's years of growth to a national network and total penetration, [t]he bootleggers and the rackets made full use of whatever was available to run their operations [Pool *et al.* 1977:28; see also Martin 1991:44-45][6].

The telephone lines, therefore, increasingly became sites of confrontation between the police and organised crime syndicates operating underground. It is often claimed that telephone surveillance was the principal method, the most frequently used tool of law enforcement agencies in their effort to enforce Prohibition measures throughout the nation (Dash *et al.* 1959:28; Diffie & Landau 1998:28).

As the telephone apparatus began to mirror the pattern of everyday life in all its expressions, law enforcement agencies found it difficult to abstain from its use. The maturing of the American police and its elevation to a specialised, professional, coherent and reliable administrative body was closely interconnected with the adoption of the telephone as its primary instrument of communication (Leonard 1938, introduction).

5.2.0. Early Wiretapping: Law and Order on the Network.

There is an important sense in which the criterion for the adoption of telephony for internal communication and co-ordination purposes is not indicative of the extent to

---

[5] In 1913, Congress enacted the Webb-Kenyon Act, which forbade the mailing or shipping of liquor into states that banned such shipments. In December 1917, the Congress approved the 18th Amendment to the Constitution, prohibiting the manufacture, sale, transportation, import and export of liquor. It was ratified by the states in January 1919 and, in October 1919, Congress adopted the Volstead Act, which provided for the nationwide enforcement of the 18th Amendment and defined 'intoxicating' liquors as those containing at least 0.5 per cent alcohol. The 18th Amendment went into effect during the following year.

[6] In the press there often surfaced accusations that criminal motives were behind large portions of telephone usage. The New York Telephone Company was accused in 1907 of earning more than 2 per cent of its annual revenues, approximately a million dollars, from telephone calls relating to gambling and other illegal operations of its users (Pool *et al.* 1977:137).

which police apparatuses in Britain and America made full use of the system.

What ought to be examined is the desire, as well as the ability, of law enforcement agencies to expand their policing function into the realm of the telephone network. As telephones became widespread, reaching businesses, offices, governments and schools, entering people's houses and appearing in public places, they gradually constituted a network of communication that penetrated the everyday functions of society –legal and illegal. It was, therefore, not long before police agencies were drawn into assuming the responsibility of supervising and maintaining law and order in the virtual domain of the electric communications network. The vehicle of this newly assumed responsibility was the practice of wiretapping.

As a concept and a practice, wiretapping dates back to the beginnings of telephony (Spindel 1968:23). As is usually the case with new and untested communications technologies, the advanced interconnectivity facilitated by the telephone was seen as threatening to penetrate not only the traditional borders of social division, but also the demarcation between the public and private spheres of existence. The active concern of telephony's customers about wiretapping can be observed in the numerous early attempts by entrepreneurs to increase telephonic privacy through the invention of various gadgets attached onto the telephone appliance. On both sides of the Atlantic, secrecy switches, jammers, voice scramblers, frequency changers, and other devices were produced and sold in large quantities. This was often done without the approval of telephone companies. The latter interpreted them as attempts to alter and distort the properties of the network by decentralising the powers of the main switching stations (Martin 1991:20ff). In 1881, there were comments in the American press that customer control over privacy would only be achieved when every user would "be his [or her] own operator" (ibid.:145). Eventually, the telephone companies managed to retain control of the network, either through legal or administrative means. According to Martin (1991),

> had the telephone companies encouraged the development of secrecy devices attached to the telephone apparatus, privacy in the telephone system would have been entirely controlled by the users, and the structure of the system might have developed in a quite different manner [Martin 1991:21-22].

The importance of wiretapping, as well as of privacy, was aptly demonstrated in warfare. During World War I, the existence of thousands of miles of field telephone cables that

crossed the battlefields of Europe, caused the formation of numerous undercover groups of intelligence agents –both allies and Germans– who wandered around central Europe penetrating enemy communication lines (Wingfield 1984:18). All sides competed in efforts to wiretap telephone cables belonging to the enemy, or protect their own, through the use of privacy devices. Enemy undercover wiretapping posts were often uncovered in Britain, the US and Germany throughout the duration of the conflict (Wingfield 1984:19; Robertson 1947:118). The paramount significance attributed to the telephone as a warfare device by the British is illustrated by the *HMS Telconia* incident, which had a tremendous impact on the course and outcome of the War. Wingfield (1984) reports that

> [o]n the very first day of the war, 5 August 1914, the British sent the cable ship *Telconia* out to the North Sea with orders to grapple for, lift and cut Germany's transatlantic cables. With this operation successfully completed, Germany was forced to communicate with distant areas of the world either by radio or by using cables controlled by her enemies [Wingfield 1984:19].

Needless to say, from day one of the war until its conclusion, intelligence agencies in both Britain and America exercised extensive domestic telegraph, telephone and mail surveillance schemes for purposes of monitoring, as well censoring, civilian communications (Porter 1987:179; Sampson 1973:35).

It would be accurate to claim that the average telephone customer was familiar with the concept of wiretapping long before World War I. It was known to early subscribers that conversations on the network were closely supervised by the companies themselves, most of whom adhered to strict policy rules regarding the use of 'vulgar or obscene language' over the telephone (Marvin 1988:88, 89[7]).

In the US, the first ever incident of systematic wiretapping by a law enforcement agency was recorded in New York City, NY, in 1894. Although initially fervently denied by police, New York Telephone Company and Western Union Telephone Company officials[8], the latter admitted in 1916 that the New York Police Department had been engaged in extensive wiretapping of telephones belonging to Catholic church institutions

[7] Based on articles in the *Electrical World* (29 November 1884) and *Scientific American* (7 November 1883). A Canadian newspaper, the *Ontario Globe*, had asserted in 1907 that the Bell Telephone Company had in its possession "the machinery for a system of espionage more than Russian in its perfection" (ctd in Martin 1991:145).

[8] A statement by Western Union said that they had "no authority to subject the messages of our patrons to the eyes of or ears of anyone else"; and continued: "[a]ny business carried on between us and the police will, as heretofore, be carried on by our usual system, by which we serve the public" (*New York Times* 3 August 1894, ctd in Dash *et al.* 1959:24).

and their members, in an attempt to collect evidence on a suspected charity fraud scandal[9].

Although few allegations of law enforcement wiretapping saw the light of publicity, it appears that, in the complete absence of public scrutiny, the New York City Police Department resorted to illegal telephone surveillance in numerous instances in the years between 1892 and 1938 (Dash *et al.* 1959, 26, 35-36). Similar in nature were the practices of police agencies in other American states during those years, including Rhode Island, Connecticut and California (ibid.:162; Marvin 1988:68).

At that time, wiretapping began to be increasingly used for purposes of political policing. Since prior to the turn of the century, police officers in New York had began wiretapping the central offices of a number of trade union organisations in the city (Dash *et al.* 1959:27). A few years later, the then primitive technology of wiretapping was "promiscuously used" (Ungar 1975:443) by the FBI. In Britain, the systematic wiretapping of the county's trade unions dates back at least to the 1926 General Strike, when the leader of the Transport Workers Union, Ernest Bevin, was targeted by the Special Branch (Fitzgerald & Leopold 1987:27[10]). Before that, the telephones of the Communist Party of Great Britain had began to be systematically monitored, shortly before the 1920s, in what some claim to have been the country's longest-running telephone surveillance operation (Andrew 1985:368).

5.3.0. The Legal Pretexts of Wiretapping.

Historically, the overwhelming majority of law enforcement wiretapping operations in Britain has been practised by three government agencies, namely the Security Service, the London Metropolitan Police and Customs and Excise (Dash *et al.* 1959:290). Since the end of the 19th century and until the late 1930s, no specific permission or authorisation was required for wiretapping. Instead, arrangements were made directly

[9] The project had been conducted with the full knowledge of senior Police officials, the telephone companies and the city's mayor, J.P Mitchell. The wiretappings appeared to have been conducted in breach of the relevant New York state laws, which explicitly outlawed the practice of telephone surveillance. During the 1916 Congregational Investigation hearings, which resulted from the uncovering of the scandal, a number of police officers testified that, throughout the duration of the wiretappings, they had overheard countless personal conversations between lawyers and their clients, doctors and their patients, as well as between husbands and wives. The hearings were abandoned with the US' entry into World War I and no disciplinary action was ever taken (Spindel 1968:23; Gill 1994:4-5; Dash *et al.* 1959:24ff; Diffie & Landau 1998:155).

[10] Citing the *Sunday London Times*, 3 February 1980.

between law enforcement and Post Office officials. More often than not, such arrangements included the interception of telephone calls by Post Office employees on behalf of the police or the Security Service. The latter acted in the understanding that such practices were not in violation of British law (Lambert 1986:208; Bunyan 1976:197; Dash *et al.* 1959:288-289).

There was, however, an apparent inconsistency between the practice of mail interception, which ever since 1663 had required written authorisation by the Home Secretary, and telephone interception, which was carried out without any ministerial oversight. It was in 1937 when this discrepancy was eradicated through a Home Office circular requiring the Home Secretary or his/her substitutes to authorise wiretapping operations by law enforcement agencies (Bunyan 1976:39; Rolph 1973:395; Dash *et al.* 1959: 288-289; Lambert 1986:208; Fitzgerald & Leopold 1987:56, 114)[11].

The procedure remained largely unchallenged throughout the Cold War, when –it is claimed– telephone surveillance was routinely used

> to ensure that no one who is known to be a member of the Communist Party or to be associated with it in such a way as to raise legitimate doubts about his or her reliability is employed in connection with work, the nature of which is vital to the security of the state [1955 *Security Service* report ctd in Dash *et al.* 1959:291].

But, in 1957, when the Metropolitan Police divulged outside of a Court of Justice the transcripts of an intercepted telephone conversation, British Prime Minister M.H. Macmillan ordered the formation of an inquiring Committee of Privy Councillors, which later became known as the *Birkett Committee* (Command 283 1957). In its findings report, the Committee candidly declared that the origins of the authority of the government executive to intercept telephonic communications was "obscure" (ibid.:§9). It was so because, although the practice of communications interception by state authorities had been systematically exercised and legally acknowledged since the 17th century, nowhere was there to be found an actual legal basis for it. In other words, "nowhere was statutory authority for the practice actually granted to the government"

[11] In Scotland and Northern Ireland similar warrants are authorised by the relevant government ministers, or senior civil servants. Wiretapping operations for defence and military intelligence purposes require warrants signed by the Foreign or Defence Secretaries (Fitzgerald & Leopold 1987:57; Statewatch 1991:2). It should be pointed out here that this warrant authorisation process was successfully challenged before the European Court of human rights in Malone v UK. This in turn triggered the UK Interception of Communications Act 1985. The case is summarised in *http://hudoc.echr.coe.int/hudoc/default.asp?Language=en&Advanced=1* by inserting the word "malone" in the search option.

(Gill 1994:164); the state appeared to possess no legal power to wiretap the telephone conversations of its citizens (Rolph 1973:395; Fitzgerald & Leopold 1987:112; Bunyan 1976:197ff; Dash *et al.* 1959:288-289).

The Committee was, therefore, compelled to conclude that, in the absence of a lucid authoritative statement outlawing communications interception by the state, CI was to be considered lawful (Lambert 1986:210; Bunyan 1976:198). Furthermore, the lengthy practice of CI was considered to imply that "the power must have been vested in the Sovereign prior to the beginning of legal memory" (E.F. Iwi, 12 June 1957, ctd in Fitzgerald & Leopold 1987:113) and no explicit statutory authorisation was thus required (Gill 1994:164)[12]. In the words of a former senior police officer, that was "another way of saying that it is unlawful but no one cares to stop it" (Rolph 1973:395).

In 1979, the legality of wiretapping was challenged again, this time by a J. Malone. The latter was charged by the London Metropolitan Police with handling stolen goods, and was presented in court with transcripts of a number of his telephone conversations with burglars, which had been intercepted by Post Office employees[13]. However, the objections of Malone's legal team were overruled by Vice Chancellor of the Chancery Division, on the grounds that, (a) there was no basis for the right to privacy in English law; (b) right of property could not be upheld in the case of telephone conversations; (c) the code of the European Convention for the Protection of Human Rights and Fundamental Freedoms was not enforceable in English courts; and (d) the absence of statutory dictums affirming the legality of wiretapping did not render the practice illegal (Gill 1994:164) [14].

---

[12] "We favour the view that [the government's right to intercept communications] rests on the power plainly recognised by the Post Office statutes as existing before the enactment of the statutes, by whatever name the power is described" (Command 283 1957:§50). This echoes a 1952 statement by the then Home Secretary, Sir D.M. Fyfe, who claimed that telephone interception "is a power which has been used by every government, of whatever political persuasion, since the telephone was invented, and is a Prerogative power" (ctd in Fitzgerald & Leopold 1987:115).

[13] *Malone v Commissioner of Police for the Metropolis* No2, 1979, A11 ER620.

[14] In 1985 the code of the European Convention for the Protection of Human Rights and Fundamental Freedoms incorporated into English law by a resolution of the European Court of Human Rights. The incorporation appeared in the form of the Interception of Communications Act 1985 (Command 9843 1985:§9), approved by the House of Commons and the House of Lords and enacted on 25 July of that year. According to the Act, communications interception warrants may be issued for purposes of (a) preventing serious crime; (b) enhancing and maintaining national security; and (c) safeguarding the economic prosperity of the nation (ibid.:§3). Any minister may issue such warrants whereas, in cases of emergency, a wiretapping operation can go ahead and seek ministerial authorisation "at the earliest possible time thereafter" (Command 7873 1980:§9). The Security Service Act 1989 came later to facilitate the interception of non-telephonic types of cable, satellite and facsimile communication (see

In the US, the comparatively speedy penetration of the telephone seems to have alerted local communities to the phenomenon of wiretapping from quite an early stage. For instance, having already outlawed telegraph wiretapping as early as 1861, the California legislature criminalised the practice of intercepting telephone communications in 1905 (Joy & Wright 1974:253; Dash *et al.* 1959:161; Westin 1962:125). By 1909, a number of other states had followed suit, including that of Washington, whose statute explicitly declared that

> every person [...] who shall intercept, read or in any manner interrupt or delay the sending of a message over any telegraph or telephone line [...] shall be guilty of a misdemeanour [ctd in Murphy 1965:112].

The federal structure of the US has given rise to a colourful mosaic of legislative views on wiretapping, with almost as many versions of them as there are states: over the years, a number of states, including New York, Maryland, Massachusetts, Nevada and Oregon, have introduced laws permitting local law enforcement agencies to wiretap under a court order. Approximately 38 states have statutes forbidding wiretapping by all persons, though most of them have not interpreted their laws as applying specifically to the police, as is the case with Illinois and Pennsylvania. Several states, such as Louisiana, have, or have had at some point in the past, laws permitting law enforcement officials to wiretap without a court order. Finally, many states allow the use in court of telephone conversations obtained by police without court approval, while some, such as Pennsylvania, Illinois and Texas, explicitly forbid such evidence from being used in criminal trials (Westin 1962:125; Maguire 1959:203; Murphy 1965:149ff; Westin 1962:153; Lapidus 1974:45)[15].

On the federal level, however, specific legislation regulating wiretapping was completely non-existent until 1968 (Carr 1998:§2.4; Lapidus 1974:11). Prior to the nation's independence from Britain, the American judicial system followed English common law, whereas, following secession, the absence of organised law enforcement from non-urban areas meant that often, cases of eavesdropping or mail-tampering were directly handled by victims (Friedman 1973:254; Seipp 1977:11; Flaherty 1989:89). In 1878, the US Supreme Court forbade the interception of first-class mail by law enforcement agencies without a court order (Diffie & Landau 1998:129). As this ruling was not extended to

---

Gill 1994:290-296 and Leigh & Lustgarten 1989 passim).

cover telephone surveillance, for many decades federal law enforcement agencies, such as the FBI, engaged in extensive unrestricted wiretapping, practised across the nation (Jeffreys 1995:199-200).

Paradoxically, the first significant challenge of this situation was affirmed, not by a politician or a human rights activist, but by a bootlegger. In 1928, crime baron R. Olmstead was the first American citizen to be convicted on primarily CI evidence. Olmstead took his case to the US Court of Appeals and from there to the Supreme Court of the US, claiming that the interception of his telephone conversations, as well as the divulgence of the transcripts of those conversations in court, infringed on his personal rights[16]. By the narrowest possible majority of 5 to 4, the Supreme Court ultimately upheld Olmstead's conviction (Maguire 1959:200; Overstreet & Overstreet 1969:127; Lapidus 1974:16; Diffie & Landau 1998:131ff; Murphy 1965:112; Westin 1962:124). The most controversial element of the decision was that, although the laws of the state of Washington –where the defendant lived and was arrested– explicitly outlawed the practice of wiretapping, the Court nonetheless accepted the transcripts of Olmstead's telephone discussions as criminal evidence. Delivering the opinion of the Court, Chief Justice W.H. Taft said that, although Washington state legislation forbade telephone interception,

> this statute does not declare that evidence obtained by such interception shall be inadmissible, and by [...] common law [...] it would not be [...]. Whether the State of Washington may prosecute and punish several officers violating this law and those [individuals] whose messages were intercepted may sue them civilly is not before us [ctd in Murphy 1965:112].

Although "never at any moment in its whole history has [a wiretapping case] commanded the approval of all members of the Supreme Court" (Maguire 1959:200), the *Olmstead v United States* precedent has, until today, served to render federal wiretapping constitutionally compatible.

The 1934 Federal Communications Act[17] came six years later to provide a basic regulatory framework for the interception of communications. Section 605 of the Act stated that "interception and divulgence" of telephone conversations was prohibited. However, hopes for tighter control over federal wiretapping practices soon disintegrated

[15] State legislation also varies in the duration permitted for CI operations (see Carr 1998:§4.137-§4.138).
[16] As stated in the 4th Amendment of the US Constitution.

when it emerged that courts throughout the nation were taking §605 to mean that a violation occurred not upon the interception, but, upon the disclosure of the conversation to outsiders (Lapidus 1974:11)[18]. It has been claimed, though not supported by evidence, that the USDoJ –the government department behind the construction of §605– deliberately left a legal window open for federal law enforcement agencies to continue wiretapping without fear of being prosecuted (ibid.). Regardless of the motives behind §605, the fact remains that it had minimal, if any, impact upon the wiretapping routines of the FBI and other federal agencies (Murphy 1965:137; Gill 1994:13; Diffie & Landau 1998:157; Carr 1998:§1.10).

The defects of §605 vexed one of the few influential adversaries of wiretapping, US Attorney General R.H. Jackson. In late February 1940, based on a recent Supreme Court ruling declaring wiretapping illegal, he issued an authoritative directive instructing all US Attorneys to refrain from initiating any prosecution that included evidence arising from intercepted telephone conversations, regardless of whether that evidence was divulged in court. On May 21, 1940, acting under pressure by FBI and other federal intelligence agencies, and with the possibility of US military involvement in Europe on the doorstep, US President F.D. Roosevelt sent Attorney General Jackson a confidential directive commanding the exception from the Attorney General's directive of cases regarding national security, namely "persons suspected of subversive activities against the government of the United States, including suspected spies", and the limitation of such cases "insofar as possible to aliens" (Roosevelt ctd in Wise 1976:98)[19].

Following World War II, the admitted excesses of the USHCUAA brought about, within government circles, a relatively comprehensive discussion on wiretapping and the right to privacy. For different reasons, participants of all sides consented that §605 was, in the words of N. Katzenbach who was then US Attorney General, "the worst of all possible solutions" (ctd in Wise 1976:22). From this consent, substantiated by a number of successful legal challenges[20], emerged Title III of the 1968 Omnibus Crime Control and

---

[17] Act of June 19, 1934, ch.652, §605, 48 Stat. 1103, as amended, 47 USC §605 (1982).

[18] The legal precedent of that was set in *Nardone v United States* 302 US 379, 58 S. Ct. 275, 82 L. Ed. 314, 1937.

[19] "You are therefore authorised and directed, in such cases as you may approve, after investigation of the need in each case, to authorise the necessary investigating agents that they are at liberty to secure information by listening devices directed to the conversations or other communications of persons suspected of subversive activities against the government of the United States, including suspected spies. You are requested furthermore to limit these investigations so as to be conducted to a minimum and to limit them in so far as possible to aliens" (Roosevelt ctd in Murphy 1965:135-136).

[20] Including Katz v US 389 US 347 (1967) and Berger v US 388 US 41 (1967).

Safe Streets Act[21], which has defined the regulatory framework of CI in the country ever since.

Title III of the Act was overwhelmingly approved in June of that year by Senate and Representative majorities. It constituted the inaugural official sanctioning of federal wiretapping in the nation's legal history. While outlawing eavesdropping of all kinds by private individuals, Title III limited the use of authorised wiretaps to the investigation of specific types of crime[22] and barred the use of unlawfully intercepted telephonic communications as evidence in court. Furthermore, it specified the procedure of warrant authorisation required for wiretapping operations and limited their maximum duration to 30 days. Wiretapping without court authorisation was also facilitated by Title III, in two cases, namely during a 48 hour emergency, and for national security[23] purposes (Carr 1998:§3.143-144; Lapidus 1974:1ff, 42; Gill 1994:15; Diffie & Landau 1998:171).

5.4.0 The Absence of Popular and Executive Control Over Wiretapping.

It is difficult to estimate the precise number of state institutions that possess and use wiretapping equipment. The overwhelmingly secretive nature of the practice means that governments are not required to inform the public about it. In the UK, local police departments, the Scotland Yard, the Secret Service –including MI5, Military Intelligence 6 (MI6) and GCHQ as well as Customs and Excise conduct their own wiretapping investigations. There is no reason, however, why other agencies, such as those concerned with quality control, safety regulations, the nuclear industry, social care or pensions, would not subscribe to the practice. In the US it is known that, apart from local and federal law enforcement agencies, the NSA, the Defence Intelligence Agency (DIA) and the Military Intelligence Agency (MIA), the Secret Service, the Internal Revenue Service (IRS) and the DoJ all possess CI capabilities (Wingfield 1984:31). With reference to the US, Lapidus (1974:12) reports that over 60 state agencies have access to telephone surveillance hardware.

Indeed, it is not improbable that, in both the UK and the US, the sheer number of state institutions, organisations, authorities, boards and agencies that possess wiretapping

[21] Title III of the Omnibus Crime Control and Safe Streets Act of June 19, 1968, Pub. L. No. 90-351, §802, 82 Stat. 212).
[22] Such as kidnapping, gambling, counterfeiting, murder, etc.

capabilities decreases the opportunities for strict executive control over the practice. In the US, for instance, many local FBI offices usually incorporate telephone monitoring studios for use by agents (Ungar 1975:188). These so-called 'radio rooms' (ibid.) are regulated and administered by the local FBI offices, and thus information as to their use remains in local files, unless there are specific reasons for them to be dispatched to the FBI headquarters in Virginia (Elliff 1972:26). Consequently, it is almost impossible for the Director of the FBI, let alone the Attorney General to become aware at any particular point in time of the exact extent of wiretapping exercised by the FBI throughout the country.

There are also further complexities, of which the US is a good case in point: a single warrant permitting telephone surveillance, in aid of a specific investigation of a suspect, can potentially be used to cover not only the target suspect him or herself, but all telephone users, organisations and institutions which may be connected to the suspect. Finally, observers have claimed that, in areas such as Northern Ireland, law enforcement and intelligence bodies have, for decades, intercepted telephone communications in the absence of adequate ministerial authorisation (Wingfield 1984:28; Lapidus 1974:6; Lambert 1986:212, 218). If all these claims are taken into account, then a picture begins to emerge of a state apparatus that often fails to keep track of its wiretapping operations. Observers have claimed that, in the past, the relaxed internal monitoring system over CI gave the FBI "free rein in collecting wide-ranging domestic intelligence" (Diffie & Landau 1998:162).

In Britain, the very concept of CI by the state is based on the often secretive and paternalistic character of the state's executive branch (Robertson 1982:22ff; Harden & Lewis 1988:ch4). Consequently, although state agencies in possession of wiretapping hardware have been required to operate on telephone surveillance quotas[24], the extent to which ministerial approval has been consistently sought by British law enforcement agencies for CI operations is often strongly disputed by observers (Gill 1994:220). Fitzgerald & Leopold (1987), for instance, report that during the Cold War, MI5 agents would usually instigate wiretapping operations upon suspicion and would proceed to apply for a warrant only if their suspicions were confirmed by the intercepted

[23] "An emergency situation exists with respect to conspiratorial activities threatening the national security interest or to conspiratorial activities characteristic of organised crime" [§2518(7)].
[24] Established and supervised solely by the Home Office Secretary (Command 108 1987:§53-§54).

conversations (Fitzgerald & Leopold 1987:57-58).

Historically, the relative –total, prior to 1986– absence of a clear legislative basis for state wiretapping in Britain has practically excluded Parliamentary control over the practice. State officials have often been extremely honest about these arrangements. Speaking in the House of Commons on 1 April 1980, the British Home Secretary candidly confessed that

> [t]he interception of communications is, by definition, a practice that depends for its effectiveness and value upon being carried out in secret and cannot, therefore, be subject to the normal processes of Parliamentary control [ctd in Lambert 1986:210].

In the US, commentators have recognised the "relative inability of Congress" to regulate state-sponsored CI as one of the most "interesting aspects" surrounding the issue (Murphy 1965:157). The periodically resurfacing National Wiretapping Commission has suggested that

> despite the Department[of Justice]'s assertions to the contrary, there is an absence of well-defined procedures which would promote compliance with the statutory standards and permit meaningful congregational scrutiny of this extraordinary executive activity [ctd in Navasky & Lewin 1973:298-289].

The USDoJ has repeatedly been accused of being unable to establish an adequate system of control over wiretapping by law enforcement agencies. On 19 June 1972, the US Supreme court decided by an eight to zero vote that a court order was required to wiretap the telephone apparatuses of US citizens who do not appear to have "significant connection with a foreign power, its agents, or agencies" (ctd in Lapidus 1974:97). Shortly afterwards, US Attorney General R.G. Kleindienst personally pledged to eliminate all illegal electronic surveillance operations. Less than a fortnight later, USDoJ officials reported to the US Congress that wiretapping of domestic radicals without apparent connections to foreign agencies was indeed continuing (Gill 1994:16). A few months later, the exposure of the Watergate scandal caused Kleindienst to resign. During the Watergate investigations, former US Attorney General R. Clark stated:

> [r]eports by FBI agents on electronic surveillance had caused the Department [of Justice] deep embarrassment many times. Often we would go to court and say that there had been no electronic surveillance and then we would find out we had been wrong. Often you could not find out what was going on [...] frequently agents lost the facts [USSSCSGORIA

1976b:337-348].

This alleged absence of democratic controls over the Cold War CI practices of US law enforcement agencies is often said to have resulted to the correlative absence of a culture of accountability and respect for democratic procedures on the part of those agencies. An illustration of this can be seen in the insistence of the Director of the NSA, in 1981, that the United States Congressional Committee on Governmental Operations (USCCGO) forwarded him a copy of its investigative report entitled *The Government's Classification of Private Ideas* prior to its official issuance. In disbelief, the Committee pointed out to the NSA that "Congress does not submit its reports to Executive Branch agencies for preview" (United States House of Representatives 1987:21-22).

5.5.0. Wiretapping in Practice.

The absence of substantial popular or, some would say, even executive oversight of domestic CI, effectively means that attempting to analyse the qualitative and quantitative aspects of government wiretapping by reference to its official, legal framework is exceedingly difficult and, usually, unproductive. The sensitivity of the practice has kept it largely concealed from popular scrutiny and the foremost executive principle guiding government-sponsored wiretapping over the years has been that of maximum operational secrecy and, often, political camouflage.

The actual extent of the use and misuse of wiretapping by state agencies may eventually come to light. At present, there is little hope for an effective and open dialogue, since "electronic surveillance is barely acknowledged by the authorities" (Lambert 1986:208). Even investigative reports, such as the 43-page account of the aforementioned Birkett Committee (Command 283 1957), arguably the most extensive official source of information on wiretapping in Britain, have been described by observers as "seriously incomplete" (Fitzgerald & Leopold 1987:120)[25].

As is the case with many official figures, the validity of governmental estimations of wiretapping differ, often dramatically, from estimations provided by independent observers. They former are thus heavily disputed. In 1954, Justice W.O. Douglas of the US Supreme Court asserted that

[25] The Birkett report has been criticised for failing to acknowledge the role of GCHQ in domestic CI, as well as that of the Foreign Secretary in authorising domestic CI operations (Command 283 1957:§53ff).

> during 1952 there were in New York City alone at least 58,000 orders issued which allowed wiretapping –over 150 a day every day in the year [Douglas 1954:355].

Yet, official figures of authorised wiretappings carried out during that very same year in the entire state of New York, claimed no more than 419 authorisations (Dash *et al.* 1959:42). In Britain, claims made by the national press that there had been almost 2,000 warrants issued to the London Metropolitan Police in 1970 and 1972, were rejected by the Minister for State, M. Carlisle, as "ludicrously high" (Bunyan 1976:201; Fitzgerald & Leopold 1987:130)[26].

5.5.1. Considerations on the Actual Extent of Wiretapping.

For decades, critics of government-sponsored CI have claimed that, during the Cold War, the absence of parliamentary control in domestic CI encouraged, if not practically directed, law enforcement agencies to use their wiretapping capabilities far in excess of legal limitations (Navaski & Lewin 1973:298-289). What is more, it is claimed that the use of wiretapping techniques has been used as aide in the lengthy and systematic abuse of human rights, including political freedom and the right to privacy[27].

More often than not, the above target is said to have been achieved through institutionalised lying and deception, "denial and related arts" (Donner 1980:24). In the US, this was first practised and, indeed, perfected by FBI Director –for 48 years– J.E. Hoover. For 34 consecutive years, from 1924 to 1957, Hoover's official attitude towards wiretapping Americans was overly negative. In public he often resorted to vocal remarks directed against the practice. In a 1931 Congressional hearing, for instance, he said:

> [w]e have a very definite rule in the Bureau that any employee engaging in wiretapping will be dismissed from the service of the Bureau [...]. While it may not be illegal, I think it is unethical, and it is not permitted under the regulations by the Attorney General [ctd in Murphy 1965:129].

And in 1939 he remarked:

> [w]hile I concede that the telephone tap is from time to time of limited value in the criminal investigation, I frankly believe that if a statute of this kind were enacted, the abuses therefrom would far outweigh the value which might accrue to law enforcement as a whole [ctd in Lapidus 1974:67].

[26] Citing the *London Times*, February 2, 1973. Carlisle refused to disclose official figures in the name of the national interest.

[27] For a discussion of the alleged legal shortcomings of US and UK domestic CI legislation see Appendix 2.

Behind the scenes, however, and, critics claim, under Hoover's full knowledge and support, the FBI was already extensively engaging in wiretapping operations as early as the early 1930s (USSSCSGORIA 1976a:12; Gill 1994:8). As is evident in the –now declassified– *FBI Manual* he actively encouraged Bureau agents to use domestic CI techniques to uncover communist influence in areas such as "political activities, Negro question, youth matters, women's matters, farmers' matters, veterans' matters" (*FBI Manual* §87:5-11, ctd in USSSCSGORIA 1976a:363). Hoover's abuses have been described by critics as "monumental" (Kessler 1993:375). Until his death, he wiretapped numerous Senators and Congresspersons, political personalities of all convictions, Supreme Court Judges, campaigners, activists and entertainers (USSSCSGORIA 1976b:313-314, 345; Murphy 1965:158). Many insist that, to cover his abuses, he deceived Congress and the American public. Allegedly, his most often-used technique was to have the majority of operating FBI wiretaps shut down for the day he presented his annual testimony to Congress so that he would not have to lie about the number of active wiretaps. He would then have them resumed on the following day (Donner 1980:24; Jeffreys 1995:200; Diffie & Landau 1998:271n; USSSCSGORIA 1976b:302).

The outbreak of World War II gave Hoover the pretext to recognise publicly for the first time that changing world developments pointed to the possible use of wiretapping for purposes of preventing espionage and sabotage by aliens (ctd in Murphy 1965:137-138). Yet, along with suspected aliens, primary targets of civilian and military intelligence wiretapping operations during World War II were –apart from the Roosevelts (Wise 1976:98n)– nuclear scientists, the Communist Party, and scores of other legal organisations, including

> the Congress of Industrial Organisations' Council and Marine Committee; the Tobacco, Agricultural, and Allied Workers of America; the International Longshoremen's and Warehousemen's Union; the National Maritime Union; the National Union of Marine Cooks and Stewards; and the United Public Workers of America [Diffie & Landau 1998:138; see also Theoharis & Cox 1988:10, 438].

The War was followed by anticommunist obsession and by an almost complete lifting of all regulatory frameworks over wiretapping. Researchers assert that, in 1948, the New York County Criminal Courts Bar reported that the New York police had reached the stage of employing wiretaps for the most minor of offences (Dash *et al.* 1959:33). On March 4, 1949, USDoJ alien registration official S.E. Coplon was arrested in New York

City by FBI agents who believed she was about to hand 28 classified FBI documents to V. Gubitchev, a member of staff of the Union of Soviet Socialist Republic's (USSR) United Nations (UN) mission. During the trials, the content of the documents was publicly disclosed, to the detriment of the FBI, after a request by Coplon's defence lawyers. The documents revealed details of an illegal FBI wiretap operation targeting pro-New Deal intellectuals E. Condon and D. Niles, and entertainers F. March and E.G. Robinson, who had publicly rebuked the USHCUAA and had expressed support for Henry Wallace's 1948 Progressive Party campaign, as well as a student writing a masters thesis on the New Deal in New Zealand (Theoharis 1978:100).

It was indeed under McCarthyism that the practice, as well as the fear of, systematic telephone surveillance spread, reaching virtually every sector of state and civil society in America. Numerous investigations conducted "by newspapers, state committees and the Senate" (Brenton 1964:163) raised strong suspicions of illegal wiretapping by local law enforcement officials throughout the country. Wiretap orders for purposes of political surveillance against individuals and groups were "obtained in quantity and in blank" (Spindel 1968:43, 202; see also Donner 1980:244; Westin 1962:152), in direct violation of federal and state laws. In New York state, for instance, official figures showed approximately 3,000 wiretap orders for the period between 1950 and 1955. However, in what is the most detailed study of wiretapping ever undertaken in the US, academic researchers Dash *et al.* (1959) concluded that, with the addition of unauthorised wiretaps operated by New York state police, the figure for that period rose to somewhere between 96,000 and 174,000 (Dash *et al.* 1959:68).

Even though declassified "[e]vidence indicates that the FBI did not believe that the Communist Party [constituted] a serious threat as it had in the 1940s" (USSSCSGORIA 1976a:66), the Party remained the primary target of illegal state-sponsored telephone surveillance throughout the 1950s (Diffie & Landau 1998:140). It seems probable, however, that equally ferocious CI operations were conducted against state officials themselves, especially those working in defence posts. For instance,

> [n]ewsman Ben H. Bagdikian, on the Washington scene for a number of years, stated in a *Saturday Evening Post* article on news managing that a considerable number of Pentagon officials take it for granted that their offices are bugged. And "almost every defence correspondent I talked to", he added, "assumed his telephone, office and home are tapped by some government agency" [Brenton 1964:164].

The 1950s also witnessed the most extensive illegal CI operation by a law enforcement agency ever exposed in the US. In February 1955, what was, in effect, an illegal wiretapping station maintained and operated by New York Police Department officers and a number of private detectives, as well as two New York Telephone Company personnel, was uncovered in downtown New York City. Through it, police officers were able to monitor more than 125,000 telephone lines on the City's East Side, including the Manhattan business sector, numerous diplomatic missions and consulates, and even the telephone network of the UN headquarters. Four people were arrested, all of whom denied operating on behalf of the FBI or other US government agencies (Spindel 1968:26, 105ff; Westin 1962:152).

Researchers claim that the resurfacing of American political radicalism during the 1960s was met by a further wave of illegal use of wiretapping operations. These wiretaps were used by law enforcement institutions either as means of neutralising radical political groups or individuals who were providing political intelligence to law enforcement executives, or simply gathering information (Donner 1980:245; Ungar 1975:449). Often, the *possibility* of communist infiltration of dissident political groups was seen as sufficient to justify warranted or unwarranted telephone surveillance operations, which often lasted for many months, some claim even years (Donner 1980:244). This justification was used to target the civil rights movement and in particular its leader and social reformer Dr. Martin Luther King, Jr. The latter was particularly targeted, even though he was fiercely critical of communism and any form of violence against the state. Initially, wiretaps were installed on King's home telephone line, and two of his office telephones. Later, and under the full knowledge of the Director of the FBI, the President of the US and the Attorney General, who authorised the wiretaps, telephone surveillance was extended to cover "King's advisers, hosts, visitors, and associates, fifteen hotel rooms where he stayed, and, it is claimed, even his pulpit" (Donner 1980:244; see also Diffie & Landau 1998:142).

Other civil rights campaigners, members of the Nation of Islam and the Organisation of Afro-American Unity, including their leaders Elijah Muhammad and Malcolm X, were also targeted. In one particular incident, an official of the Nation of Islam with blank criminal record was constantly wiretapped for no fewer than 8 years, but never prosecuted (USSSCSGORIA 1976a:63).

The 1970s entered with an amusing incident in which members of a dissident group called the Citizens Commission to Investigate the FBI broke into the Bureau's district office in Media, PA, and acquired –and later distributing to the press– classified documents of telephone surveillance of politically active citizens "without evidence of wrongdoing" (Lapidus 1974:69). In a separate development in June 1971, Justice Douglas of the US Supreme Court stated that, on average, unwarranted 'national security' wiretaps lasted for 78 to 209 days, as opposed to an average of 13 days for authorised wiretaps (ibid.:101).

All wiretapping scandals that were exposed during that decade were inevitably diminished by the shadow of Watergate. US President R.M. Nixon often liked to stress his supposed curbing on unauthorised wiretapping by state agencies. In March 1971, for instance, he reported to the Senate:

> in the two years that we have been in office, now get this number, the total number of taps for national security purposes by the FBI, and I know because I look not at the information but at the decisions that are made –the total number of taps is less, has been less, than fifty a year [ctd in Gill 1994:22].

In 1973, on the very first full day of his second administration as President, Nixon ensured reporters that his entrusted US Attorney General, J.N. Mitchell –later convicted over Watergate– would govern telephone surveillance "with an iron hand" (White 1975:125). And yet, the first illegal wiretappings by Nixon and his collaborators were to begin less than 4 months after that comment[28]. After Nixon's resignation, the Church Committee, a body of US Senators who conducted a detailed, year-long investigation of domestic surveillance by intelligence and law enforcement agencies, characteristically reported that the nature, extent and pernicious nature of domestic intelligence operations "threaten to undermine our democratic society and fundamentally alter its nature" (USSSCSGORIA 1976a:1).

In Britain, there has been comparatively little evidence of actual instances of wiretapping

[28] Along with Watergate, the Nixon administration was responsible for another sinister scheme involving wiretapping, often called Huston Plan, after its designer, White House member of staff T. Huston. In a detailed report to the President, Huston suggested the "connection between domestic unrest and foreign movements and had a plan in which the resources of the CIA, the DIA, the FBI and the NSA were to be pooled to fight domestic unrest. NSA (contrary to law) would intercept communications of US citizens using international facilities. Rules regarding mail interception, electronic surveillance, and surreptitious entry would be relaxed [...]. That the Huston plan came within a hairsbreadth of being national policy shocked the nation when it was revealed several years later" (Diffie & Landau 1998:145-146).

misuse by the authorities. Yet, critics claim that the reasons have less to do with a higher respect by intelligence and law enforcement agencies for privacy and more with the traditional secrecy of the British state, as well as the equally traditional institutional intimacy between the police, the CID[29], the Special Branch, the Post Office and BT, Britain's foremost telephone service provider –of which more later[30]. Official documents by successive British governments view state-sponsored wiretapping as a marginal activity which law enforcement agencies strive to avoid as much as possible, but ultimately resort to it "from time to time" (Gill 1994:168; Command 283 1957 passim).

In theory, state agencies with access to wiretapping hardware operate according to quotas, which allow them to conduct a certain amount of wiretapping operations every year (Command 108 1987:§53-54). Official tables were published by Conservative governments throughout the 1980s. These tables contain the interceptions of communication of all kinds, authorised by the Home secretary and –to a lesser extent– the Scottish as well as the Foreign Secretaries for England, Scotland and Wales, from 1937 to 1989 (Command 7873 1980; Command 9843 1985; Gill 1994:168). Critics have indicated that the statistics contained in these tables have remained "surprisingly stable" (Lambert 1986:212), at under 600 a year, while from 1969 to 1989, wiretapping authorisations have never exceeded a total of 470 (Gill 1994:168). What tends to make independent observers view these figures distrustfully is the fact that during those 20 years the number of telephone lines in Britain has increased by 250%, from 8 to 20 million (ibid.). According to investigative journalists P. Fitzgerald and M. Leopold (1987),

> the number of warrants quoted in the White Paper bears little relation to the number of phone calls tapped by the authorities. Far more tapping goes on than has ever been admitted. [Besides the fact that] the numbers of warrants signed by the Northern Ireland Secretary, which may include taps in mainland Britain, have never been released [...], the [official] figures relate to those warrants *signed* in a particular year, not to those *in force* during that year. Warrants only stay in force for a matter of months, but they may be renewed indefinitely[31]. Many of those signed in previous years may, therefore, still be operative [Fitzgerald & Leopold 1987:14].

[29] Also known as C11.

[30] In 1985, John McWilliam MP, a former telecommunications engineer, stated in Parliament that "[i]t is wrong to say that interception has not happened without warrants. In addition to officially authorised taps certain official tappings do not require warrants. That derives from an institutional relationship between the police, the CID or the Special Branch, and the Post Office –subsequently British Telecom" (ctd in Fitzgerald & Leopold 1987:15).

[31] "A former Home Secretary, Merlyn Rees, told the Commons in 1985 that '[s]ome taps continue for a long time. I do not intend to spell it out, even in this House. However, I imagine that every Hon[ourable] member knows what I am talking about. They are blanket tappings" (ctd in Fitzgerald & Leopold 1987:33).

In addition, critics argue, it is possible that, similar to the US, a single warrant permitting telephone surveillance in aid of a specific investigation of a suspect can potentially be used to cover not only the target suspect himself or herself, but all telephone users, organisations and institutions which may be connected with him or her (Fitzgerald & Leopold 1987:15; Gill 1994:168-169). Finally, it has often been alleged in Parliamentary debates –though never substantiated with evidence– that "[t]he problem is not phone taps authorised by the Secretary of State, it is the very much larger number of phone taps that are made without any application for an authorisation" (Ian Mikardo MP, 1985, ctd in Fitzgerald & Leopold 1987:15). Critics appear convinced that, during the Cold War, lengthy state-sponsored CI operations were conducted against the CP, the National Council for Civil Liberties (NCCL, today known as Liberty), the CND, left-wing and ultra-right wing groups and organisations of all persuasions, environmental pressure groups, nationalist parties such as Plaid Cymru and the Scottish Nationalist Party (SNP), as well as numerous Labour Party politicians and members (Fitzgerald & Leopold 1987:33ff[32]).

In the alleged absence of concrete and trustworthy data, logical inference has been a tool often utilised by researchers. Wingfield (1984), for instance, claims that the less than 500 wiretapping orders *per annum* is a number that does not justify the sheer size of agencies solely concerned with communications interception in Britain. In 1982, he continues, it was reported that one state-sponsored telephone surveillance site in London employed over 100 technicians and operated on an annual budget of £1¼ million (Wingfield 1984:28). Others further this position by stating that, by the late 1980s, GCHQ employed 11,500 full time staff, including 7,000 civilians and 4,500 service personnel (Fitzgerald & Leopold 1987:48; Norton-Taylor 1990:53). To that, Gill (1994) insists, one should add the wiretapping facilities maintained and operated by BT itself. By the mid 1990s, the company had

> 60 full-time tapping operatives [as well as] 80 higher grade engineers maintaining and servicing tapped lines. At the BT centre in Gresham Street there are more than 1,000 lines plus switching mechanisms [...] deal[ing] with many thousands of incoming intercepts. [The centre was staffed by] 100 transcribers while [a]dditional transcribers work[ed] at MI5 on the material directed there [Gill 1994:167].

Clearly, critics conclude, the *potential* indicated by the technical and administrative capacity of British governmental agencies has been, and remains, much greater than the official disclosures of the extent of wiretapping operations in the country.

[32] Northern Ireland is not included in this account.

5.6.0. The Law Enforcement–Telecommunications Interface.

The practice of CI is not politically sensitive only because it evades privacy, but also because it represents one of the few functions of intelligence and law enforcement agencies which involve the co-operation and approval of non-governmental agencies – namely the telephone carriers. In reality, it has not been necessary for intelligence investigators to rely on the assistance of the telephone companies for the execution of wiretapping operations. In the days when most telephone cables could still be visibly traced in public areas, basic equipment such as a pair of pliers, a wire and a pair of headphones could be used to wiretap a target line from the local telephone junction box – the most accessible interception point in the local network. From the standpoint of security, however, such operations have usually been problematic. In the words of a Post Office Engineering (1980) report, wiretaps installed at local telephone junctions "present formidable technical and practical problems [and are] too open to public view and too liable to discovery by Post Office engineers on normal duties" (Post Office Engineering Union 1980:20).

Additionally, the acceleration in the development of telephone technology, especially after World War II , has made the task of wiretapping immensely more complex over the years, even prior to digitisation. Identifying the telephone number of a target suspect is based on information available even to the average subscriber, through the *White Pages*; but as telephone lines are usually strung together in bunches of up to 100, identifying the particular telephone cable and pair at the junction box is practically impossible without access to expert knowledge and specialised technical data available only to the telephone company, and used by linemen on the job (Brenton 1964:160; Dash *et al.* 1959:66, 293; Lapidus 1974:124). These complex security and technical problems can only be eliminated with the direct and substantial co-operation of the telephone carrier. Ideally, wiretaps are installed and maintained on the main distribution frame at the local telephone exchange or at the central telephone offices.

The necessary link ensuring the smooth and efficient co-operation between state intelligence and law enforcement agencies, on the one hand, and CSPs, on the other, is intimate institutional relations, that is, reliable "institutional arrangements" (Bunyan 1976:202) between those establishments. In countries such as Britain, France or Italy, where telephone carriers have been owned and directly controlled by the state for many

decades, those institutions have traditionally formed close functional relationships, which have played a major role in the systematic exercise of CI (Plate & Darvi 1981; Fitzgerald & Leopold 1987:9).

Critics have suggested that, historically, in both Britain and the US getting telephone company assistance for authorised wiretapping operations "is easier than getting a dial tone" (Gill 1994:23; see also Wise 1976:37n). Upon display of a valid communications interception warrant, telephone companies provide intelligence agents with either a leased line transferring targeted telephone conversations to a monitoring location, or with actual wiretapping instruments which can be used on telephone company premises. The company is eventually compensated for its expenses by the agencies concerned (Carr 1998:§127-128; Diffie & Landau 1998:172; Lapidus 1974:124). But unauthorised wiretapping, which, critics claim, has historically been much more extensive than authorised wiretapping by state agencies, depends almost completely on telephone company assistance (Dash *et al.* 1959:72, 293).

In Britain, the history of institutional intimacy between organised law enforcement agencies and CSPs was initiated on the very year of the establishment of the London Metropolitan Police. At that time, the Confidential Enquiry Branch was formed and assigned the task of supervising the content of suspicious correspondence distributed by the Post Office (Petrow 1994:264). During the late 19th century, under the directions of the Metropolitan Police Assistant Commissioner, the Branch utilised its position inside the Post Office to initiate a passionate crusade against the increasing use of the mail and telephone for gambling and prostitution[33].

In an instance illustrative of the complex nature of cross-departmental negotiation, the Post Office refused to co-operate with the London Metropolitan Police by forbidding its officers to intercept the communications of British citizens. The Post Office Solicitor, Sir R. Hunter, protested that he was a carrier of messages, not "a censor of public morals" (ctd in Petrow 1994:266). In a fierce response, H.B. Simpson of the Home Office accused Sir Hunter of being

> a carrier who actually ascertains or might with ordinary intelligence easily ascertain that his services are being used for an illegal purpose [and he, therefore, could not avoid] criminal responsibility [ctd ibid.].

[33] Discussed earlier in section 4.1.3. n24.

But the uncooperative attitude of the Post Office continued. In 1897, the Postmaster General, the Duke of Norfolk, announced that he could not assist the police unless empowered by Parliament (ibid.). In 1906, his successor, Postmaster General S. Buxton, insisted that sufficient policing of the telephone network implied nothing less of "a general censorship" of all conversations, something which he found unacceptable (ibid.:270). Eventually, the Home Office was able to completely succumb the resistance of the Post Office by resorting to the appointment of H. Samuel, a public administrator favourable to the CI mandates of the Metropolitan Police, to the post of Postmaster General, in 1910 (ibid.:268).

During the same year, the newly-founded MI5 was busy establishing "valuable contacts" (Fitzgerald & Leopold 1987:26) with the Post Office, and arranging the facilitation of postal and telephonic surveillance. W. Thompson, a former inspector involved in the formation of the organisation, wrote during that time that "whereas the ordinary detective can always feel that the Law stands firmly behind him, the Special more often than not lacks this advantage" (ctd in Porter 1987:176). This peculiar institutional approval of illegality governed the relationship between British intelligence agencies and the Post Office, with regard to telephone surveillance, until 1937. Up until that year, not only did the Post Office directly negotiate with MI5, the Special Branch and the police, permitting the interception of telephone communications, but it also performed such tasks on behalf of those agencies (Rolph 1973:395; Bunyan 1976:197; Fitzgerald & Leopold 1987:113-114):

> [it] maintained a separate Telephone Interception Unit, which liaised [sic] directly with MI5's counter-espionage division and transcribed conversations on its behalf from recordings made on wax-coated cylinders [ibid.:64-5].

Following World War II, the Post Office transcribers were permanently absorbed by MI5 and placed in the agency's Section A3[34] (West 1983a:18-19).

Following 1937, when the requirement of a warrant for intercepting telephone communications became a standardised process, every Post Office official had the right to refuse co-operation with the authorities unless (and sometimes even if) a valid warrant was displayed. The extent to which this right was put to use is, however, questionable, considering that the organic institutional intimacy between intelligence agencies and the

[34] The MI5's administrative and technical division, later renamed A2A.

Post Office had already been functional for almost three decades. In other words, it is very likely that the majority of law enforcement agents

> inclined simply to ignore the warrant system and make a direct approach to the G[eneral] P[ost] O[ffice], via the area head of the Post Office Investigation Division[35] (Fitzgerald & Leopold 1987:58).

One area of co-operation, which was totally unaffected by the 1937 change in legislation, was the monitoring and recording of telephone conversations conducted by Post Office employees on behalf of intelligence agents. There were numerous reports of instances of BT local exchange buildings incorporating monitoring stations staffed by company employees who routinely intercepted, recorded and even transcribed telephone conversations on behalf of law enforcement agents (Bunyan 1976:202; Fitzgerald & Leopold 1987:63-64) [36]. These arrangements were persisting by the time of the appearance of a 1969 Home Office circular[37], which stated that

> if the police are in urgent need of information which the Post Office may be able to furnish in connection with a serious criminal offence, the police officer in charge of the investigation should communicate with the Duty Officer, Post Office Investigation Division who will be ready to make any necessary inquiries [Home Office 1977:§1.70; see also Leigh 1975:215ff].

This statement, which was seen at the time as diminishing the right of refusal by the Post Office and BT to collaborate with law enforcement agencies, was accompanied a few months later by a series of ministerial decisions regarding the relationship between the General Post Office and GCHQ. Namely, the government proceeded to announce the establishment of a newly integrated communications interception complex, created under the technical co-operation of the two organisations. Technical improvements included the facilitation of immediate redirection by BT to GCHQ of targeted telephone conversations from anywhere in Britain (Fitzgerald & Leopold 1987:68[38]).

---

[35] The POID has been historically the principal point of interface between the Post Office and law enforcement and intelligence agencies. Although it operates under the control of the latter, its members are usually recruited from the ranks of former police or intelligence officers, while a minority consists of telephone technicians and engineers. Since the privatisation of British Telecom in 1981, the group has been renamed to British Telecom Investigation Department (BTID). It is staffed by approximately 300 employees.

[36] This was the case in 1952, when local councillors visiting the local BT exchange in Slough, Berkshire, were shown a fully equipped and operational listening post by a fellow councillor who was also an employee at the site (Bunyan 1976:203). In 1979, during the case of *Malone v Commissioner of Police for the Metropolis No2* (1979, A11 ER620) it was revealed that Post Office employees had intercepted and recorded telephone conversations upon the display of a warrant by the London Metropolitan Police (Lambert 1986:209).

[37] Amended and reissued in 1977.

[38] Citing the *New Statesman* of 1 February and the *London Times* of 3 February 1980.

In 1981, along with the privatisation of BT by the Conservative government, a new requirement for the company's employees was introduced: they all had to sign the Official Secrets Act which, among other things, penalised employees for any public disclosure of information relating to wiretapping practices (Fitzgerald & Leopold 1987:30[39]). Here is how Fitzgerald & Leopold (1987) view the way in which BT's privatisation has impacted on its co-operation with law enforcement:

> [u]niquely for a private company, BT now has a vital, integral role within the British intelligence complex. Should BT ever do the unthinkable, and suddenly refuse to co-operate with official telephone tapping, the government has the safety net of a 'national security' clause, written into the privatisation law [...]. Section 94 of the 1984 Telecommunications Act allows for a Secretary of State to issue BT and any other telecom[munication]s companies with such general or specific directives "as appear to the Secretary of State to be requisite or expedient in the interests of national security". The directive must be implemented, continues the section, irrespective of other obligations (to shareholders, for instance). Other clauses permit the Secretary to withhold the directive from Parliament "in the interests of national security" and to reimburse the carriers for the cost of complying with the directive. The carriers are prevented from revealing the fact or substance of any such directive [Fitzgerald & Leopold 1987:82].

In the US there has been little evidence of early involvement of organised law enforcement agencies in the everyday running of the Bell Telephone company. The closest example is the coercion imposed on the company in 1902 by the Canadian government to allow "peace officers" to search for irregularities in the records of telephone subscribers. It remains uncertain, however, whether records of customers in the US were searched during that operation (Martin 1991:44). The first recorded instance of a "loose arrangement" (Dash *et al.* 1959:25) between a law enforcement agency and a telephone company occurred in 1895, in New York City, NY, where the local carrier systematically assisted the police department in its wiretapping operations during a fraud investigation (ibid.[40]). But, on the whole, there is an absence of significant evidence of intimate collaboration between law enforcement agencies and telephone companies during the early decades of the 20th century. Critics assert that this leads one to believe that it was primarily the personal connections between intelligence officers and telephone company employees that provided isolated areas of functional overlap.

It was during World War II that this overlay was refined and, gradually, institutionalised.

---

[39] Citing from the *Guardian*, 3 May 1984.

Naval intelligence requested that the Record Company of America (RCA) Global provide copies of all Japanese cable traffic to and from the island of Hawaii. Additionally, virtually all international telegraph messages carried by RCA Global, IT&T World Communications and Western Union International were intercepted by military officers throughout the duration of the War (Theoharis 1978:120). The intimate institutional settings facilitated during those exercises permitted their continuation after the formal end of World War II. In August 1945, military intelligence expressed interest in retaining post-war access to messages of foreign governments carried by the three aforementioned corporations. The companies accepted after having secured formal assurances by no other than US Attorney General T. Clark and Defence Secretary J. Forestal that they would be legally protected even though their consent to allow intelligence interception of cable traffic was in direct violation of §605 of the 1934 Federal Communications Act (ibid.)[41]. During the Cold War, this institutional intimacy proved invaluable for intelligence authorities. Through it, the NSA managed to obtain access to cable traffic carried by Western Union, RCA, and IT&T to and from selected domestic and international intelligence targets (USSSCSGORIA 1976a:108).

During that time, the telephone companies' disclosure of telephone information to law enforcement agencies was rarely challenged under §605[42], and rarely effectively[43] (Carr 1998:§1.13-14) . All possibilities for successfully challenging that activity were eventually diminished in 1970, with the amendment of Title III of the Omnibus Crime Control and Safe Streets Act. Under §2511(2)(a)(ii) of the amended Title[44], telephone companies were required by law to provide the necessary information and technical assistance to authorised law enforcement agents. The 1970 amendment had been the USDoJ's response to an earlier incident in which the Nevada Telephone Company had refused to assist intelligence officers in performing a wiretap. Five years earlier, the company had been subjected to a US$6 million lawsuit for assisting an FBI-sponsored wiretapping operation (Carr 1998:§3.76-§3.77; Lapidus 1974:123).

This incident directs us, once again, to the complexity of the institutional forces in question. Despite assertions by critics, it would be factual inaccuracy and political

---

[40] Citing the *New York Times* of 18 March 1916.
[41] This scheme, officially known as operation Shamrock, was maintained until 15 March 1975, when it was uncovered by the press.
[42] For instance, in *Brandon v United States* 1941 and *Bubis v United States* 1967.
[43] Such as in *United States v Caplan* 1966.

oversimplification to claim that the telephone companies have historically been prepared to consent to their role as aides to state wiretapping operations. Sporadic in number, yet significant in symbolic value, refusals by companies to co-operate with the authorities have been recorded during the Cold War and even after the application of the 1970 amendment to §2518(4) (Carr 1998:§4.127; Dash *et al.* 1959). Such refusals do indeed make logical sense: systematic assaults on the privacy of telephone users can undermine the status of the network and, in turn, the revenue of the carrier (Brenton 1964:162). It should not, therefore, be surprising that, ever since World War II, American telephone companies have been very stringent in the internal policing of their employees, who are continuously "exhorted on the theme of communications secrecy and made fully cognisant of state and federal laws dealing with the subject" (Brenton 1964:162-163; see also Lapidus 1974:125).

Equally predictable has been the persistent support by the telephone companies of rules and regulations that enhance the privacy of their customers. As early as 1928, in *Olmstead v United States*[45] a group of the largest telephone companies in the country presented an *amicus curiæ*[46] in support of Olmstead, in which it was asserted that any form of wiretapping "violates the property rights of both persons using the telephone" (ctd in Murphy 1965:89-90). In 1963, W. Powell, an influential New York Telephone Company executive, openly stated his complete disapproval of any form of invasion of the privacy of telephone users irrespective of the reasons behind it (Brenton 1964:162). Four years later, on May 18, 1967, during the official hearings on privacy invasion held by the US Senate Subcommittee on Administrative Practice and Procedure, the Vice President of AT&T declared that the Bell System supported a complete and general outlawing of all wiretapping, with the exception of interceptions performed on national security grounds:

> [p]rivacy of communications is a basic concept in our business. We believe the public has an inherent right to feel that they can use the telephone with confidence, just as they talk face to face. Any undermining of this confidence would seriously impair the usefulness and value of telephone communications [ctd in Lapidus 1974:126].

Bound by legal and institutional obligations towards the state, however, the telephone

[44] Public Law 91-358, Title II, Section 211(b), July 29, 1970, 84 Stat. 654.
[45] Already discussed earlier, in section 5.3.0.

industry has been largely unable to, on the one hand, enjoy the state's preferential treatment while, on the other hand, protecting the privacy features of its communications networks from interference by state agencies. It has learned to negotiate and protect its interests within the existing legal and institutional framework. For the most part, the telephone companies are "happy to be let off the hook" (Lapidus 1974:123-124). Their dealings with law enforcement agencies are, for the most part, friendly and business-like (Dash *et al.* 1959:246). They assist the latter while striving to maintain a form of functional neutrality:

> [w]e try to minimise our role to the greatest extent. The less we know, the better, from the standpoint of law enforcement. The primary interest of the Bell System is the preservation of secrecy of communications to the maximum extent compatible with the public interest. Whether or not law enforcement officers should wiretap is a question for Congress to determine on a balancing of interests. Since Congress has passed Title III authorising court-ordered eavesdropping, the Telephone Company accepts the law and assumes that it is constitutional [New York City Bell System official, ctd in Lapidus 1974:123-124].

On balance, the attitude of the American telephone industry toward wiretapping has not historically favoured the protection of the privacy of users. There have indeed been instances where, upon discovery of illegal state-sponsored wiretapping performed under the assistance and supervision of company employees, the latter have immediately been discharged (Dash *et al.* 1959:246). Yet, the very necessity of maintaining public confidence in the telephone system has led the companies to conceal the existence of legal and illegal CI, instead of exposing it. There has never in the history of wiretapping been an instance when a UK or US telephone company has reported an illegal telephone surveillance operation by government agencies, though many were carried out during the Cold War. In fact, it has been asserted that the general practice of law enforcement using wiretapping as an investigative lead, as opposed to evidence in court, has not been the product of legal requirements. Rather, it is said to derive from the constant demands by telephone companies to conceal the actual extent of wiretapping, thus maintaining public confidence in the telephone network (Dash *et al.* 1959:122-123, 146, 250).

Predictably, the dynamics of this situation have resulted to numerous instances in which telephone companies and their employees have repeatedly acted as agents of law

[46] A *friend of the court*. An official statement by a third party not directly related to the case, but whose interests can potentially be affected by the court's decision.

enforcement and intelligence apparatuses. Throughout the 1950s, telephone company staff in Philadelphia, PA, Boston, MA, San Francisco, CA, Chicago, IL, as well as in a number of cities in Louisiana, were consistently required to provided local and federal intelligence officers with confidential subscriber information, temporary lines for wiretapping purposes, and even recordings of telephone conversations (Dash *et al.* 1959:123, 154, 165-166, 218-220, 246). Countless such instances were also reported during the 1960s. They included the case of C.V. Gris, a New York Telephone Company employee who, along with other colleagues of his, ran for two years a sort of informal – and unquestionably illegal– wiretapping school for members of the police department, using telephone company facilities, equipment, and even money (Spindel 1968:112ff). In 1971, it was revealed that H.R. Hampton, member of the executive board of the Washington, DC-based Chesapeake & Potomac Telephone Company and Director of government Communications Services, had perceived as his "patriotic duty" to arrange tens of thousands of unauthorised CI operations for the FBI for more than 20 years prior to his retirement (Wise 1976:37-38n; Joy & Wright 1974:257). Further enquiries into the matter revealed in 1975 that the Vice Squad of the Baltimore Police Department in Maryland

> had monitored telephone conversations with co-operation from the Chesapeake and Potomac [...] Telephone Company without proper legal authorisation [...]. Staff of the C&P Security Office provided members of local and state law enforcement agencies with non-published telephone listings upon oral request until October 10, 1973 [American Friends Service Committee 1979:53].

Similar evidences emerged throughout the 1970s with regard to the underground connections between local telephone companies and FBI branches in a number of states (Ungar 1975:448).

Another service by CSPs, which US law enforcement agencies have come to expect over the years, has been alerting them whenever a complaint is received by a subscriber who suspects that their telephone line has been wiretapped. Critics claim that, during the Cold War, this constituted standard practice with authorised or 'national security' wiretappings (Brenton 1964:163; Spindel 1968:220; Dash *et* al. 1959:123). E. Belter, the Chief Supervisor of national security wiretaps for more than 20 years, explained in an interview following his retirement that, when a telephone company received a complaint from a customer who insisted that their line was wiretapped, they would inform the

agents responsible. Then, "[w]hen it was cleared up [they] would say 'Okay, it can go back on'" (ctd in Wise 1976:53-54). Carroll (1969) asserts that, during the late 1960s, the situation had reached the stage where victims of wiretapping were advised by experts not to complain to the telephone company or the police, but to use privacy-enhancing instruments instead, such as voice scramblers (Carroll 1969:163-164).

Historically, the institutional ties between telephone companies and law enforcement agencies have also been maintained through the training of officers and the sharing of surveillance technology. Even before World War II, police and intelligence officers often enrolled for courses and seminars organised by local telephone companies for their own staff (Leonard 1938:64; Dash *et al.* 1959:72). After World War II, it became customary for police and FBI CI specialists to be recruited from the ranks of former telephone company technicians, repairmen and linemen with many years' experience on the job (Dash *et al.* 1959:50, 51, 223). In addition, the wiretapping apparatus used by police and intelligence officers is often manufactured, tested and sold to them by the telephone companies themselves (ibid.:222-3, Leonard 1938:64).

5.7.0. Discussion: A Debate that Isn't.

One of the most frustrating elements of the domestic CI debate is that it is essentially not a dialogue: on the one hand, vocal critics of the practice insist on their claims. On the other hand, Home Office, or State or Justice Department officials usually resist being drawn into a discussion about the social, political or moral grounds of CI. Intelligence officials are legally forbidden from entering the debate, while law enforcement officers simply refer enquirers to the law.

The few official responses to criticism over CI centre on attempts to rationalise it, to reconcile its somewhat unpopular nature with the more healthy political characteristics of our parliamentary democracies. Such attempts are usually threefold. Firstly, there is the argument that CI is inevitable. Every state does it. Throughout the 20th century, electric and, later, electronic communications have been inseparable parts of everyday social processes, and as such, they have to be policed. Secondly, it is proposed that law-abiding citizens, who exercise their constitutional rights and obligations while respecting those of other people, have nothing to fear, because they have nothing to hide. Finally, state-sponsored wiretapping is often seen not as a right, but rather as an obligation –

namely, the obligation of modern nation-states to ensure the welfare of their citizens and other residents.

On the other side of the debate, critics argue that there is something fundamentally wrong with models of state policing, or protection, which are not subjected to popular control and accountability. In the UK and the US, centralised institutions such as law enforcement and, especially, intelligence agencies are not subjected to direct electoral control. Furthermore, they have developed within a peculiar culture of bureaucratic exclusivity and institutional autonomy, in which notions of administrative transparency, political openness and moral self-evaluation[47] have, for the most part, been regarded as weaknesses, rather than strengths. The idea that those institutions should be entrusted with the ability to invade the privacy of citizens, while, at the same time, operating under the considerable absence of popular and even executive forms of democratic control, is therefore seen as deeply problematic[48].

Wiretapping, critics assert, is not inevitable. There are many states around the world, which have been known to have either outlawed it altogether or practised it in conditions of strict legal and administrative control. Indeed, in Belgium, a country deeply involved in the Cold War, state employees are heavily penalised for conducting wiretapping or for divulging not only the content of a call, but "even metering information, such as the frequency, time and duration of calls, or the numbers dialled from a particular line" (Fitzgerald & Leopold 1987:158). The penalties stipulated in the legislation –enacted in 1930– are substantially heavier for state employees than for ordinary citizens found engaging in wiretapping. During the 1950s, New Zealand enacted a similar legislation. In 1957, the country's Postmaster General stated in the House of Representatives:

> there is no telephone tapping in this country with one exception, and that is on the authority of the Prime Minister where the national security may be involved. In those circumstances and those circumstances only, will

[47] Relevant here are the words of former FBI Assistant Director W. Sullivan, in his statement before the Church Committee in the US Senate, in November 1975: "during the ten years that I was on the US Intelligence Board [...] never once did I hear anybody, including myself, raise the question: 'is this course of action which we have agreed upon lawful, is it legal, is it ethical or moral?'. We never gave any thought to this realm of reasoning, because we were just naturally pragmatists. The one thing we were concerned about was this: will this course of action work, will it get us what we want, will we reach the objective we desire to reach?" (ctd in Theoharis 1978:94).

[48] According to Gill (1994:39) "there is inadequate democratic control of state structures in the UK, particularly of the security intelligence agencies, and [...] this poses such a threat to democratic forms that it requires fundamental change".

> telephone tapping be tolerated. For the purpose of ordinary criminal administration there will be no telephone tapping [Dash *et al.* 1959:300].

Clearly, critics exclaim, systematic wiretapping is not inevitable. In reality, it is a conscious political decision, largely shaped by the extent to which moral and political notions of respect of individual privacy inform state policy.

The argument that law-abiding citizens have nothing to fear is simply dismissed by critics, who refer to the historical instances of political abuse of CI during the Cold War. It becomes clear, they insist, from the history of wiretapping during the 20th century, that the practice has been repeatedly used against law-abiding individuals and organisations. Socialists, civil rights activists, pacifists, trade unionists, politicians, lawyers, actors, artists, feminists, students, homosexuals and environmentalists have, in the past, been repeatedly wiretapped by British and American intelligence agencies, not for judicial, but for political purposes. Often, membership in a particular organisation –as in the case of the Congress for Racial Equality in the US– standing for local or national elections –as in the case of the American Socialist Workers Party–, or even protesting against nuclear power –as in the case of the CND in Britain–, have been sufficient to justify lengthy wiretapping operations against individuals or groups. In the eyes of critics, the history of state-sponsored CI is the history of the undue invasion of privacy.

Ultimately, it would be erroneous to compare the social and political dynamics of the UK and the US during the Cold War with those of today as an attempt to dismiss the practice of CI on political grounds. Yet the unfortunate precedence of that era of heavy political tension understandably haunts the contemporary debate on CI and cannot –or, indeed, should not– be ignored.

5.8.0 Summary.

Soon after the emergence of telephony, its interconnection with everyday social negotiation was so drastic that neither the British, nor the American law enforcement apparatuses were able to ignore the impact of its uses. On both sides of the Atlantic, the responsibilities of law enforcement and intelligence organisations were sooner or later expanded to cover the policing of telephony. This expansion was indeed influenced by the peculiarities of the political landscape in each country. Thus, wiretapping acquired

more openly aggressive characteristics in the US –especially under Hooverism and McCartyism– while in the UK it assumed the discrete tone of many another governmental activity. Yet in both nations, critics have not hesitated to virtually associate the history of wiretapping with the history of the undue invasion of privacy duiring the past 100 years. The debate is inevitably marked by political and ideological polarisation, as well as by the absence of basic information. There is, however, one particular issue that might be drawn from it: the single fundamental factor which has historically facilitated the extensive use and, critics argue, misuse of wiretapping by law enforcement agencies in the UK and the US, has been the close formal and informal institutional relationship of those agencies with telephone companies and the telephone industry as a whole. This institutional interface is so critical, that any blueprint aiming toward the enhancement of the individual's right to privacy in the information society is destined to be a disappointing failure unless it addresses this tacit link between law enforcement and service providers.

Part III
EXPLORING THE CONTEMPORARY FRAMEWORK

Chapter Six

The Techniques of Interception

6.0.0. Introduction.

This chapter considers the technical basics of CI, both prior to and following the enactment of RIPA and CALEA. Apart from providing crucial technical background to the issue of CI, it explains in detail the technological reasons[1] that led to the emergence of RIPA and CALEA, as well as the structural changes that digital wiretapping poses for telecommunications and for the actors involved in it. After a brief description of the technology of analogue wiretapping, there will unfold an account of the barriers to CI that telecommunications digitisation has posed or appears likely to pose. Finally, changes in CI in the digital telecommunications environment –as facilitated by RIPA and CALEA– will be outlined and discussed[2].

6.1.0. The Micro-Mechanics of Analogue CI.

The basics of CI practice in the UK and the US Plain Old Telephone System (POTS) environments has changed little since the emergence of telephony. In most cases, a CI

[1] It should be pointed out that in RIPA's case the aim of the legislation was not only to bridge the digital technological gap that curtailed the state's CI operations, but also –some say primarily– to ensure that certain investigatory operations were properly regulated and in compliance with the Human Rights Act 1998.

[2] The technical basis and background for this chapter comes from my own knowledge of the subject, tested against a number of sources from the technical literature on CI, including Tsailovich 1999; Larsen 1997; Goralski & Kolon 2000; and Pollock 1973. The technical validity of this chapter has also been examined and verified by Dr Apostolos Georgiadis, Research Fellow at Edinburgh University's Department of Electrical Engineering (see 'Acknowledgements').

operation begins with a law enforcement or intelligence officer securing legal authorisation for intercepting communications data or content. In the UK this is usually done under the Wireless Telegraphy Acts 1949/1998 or the Interception of Communications Act 1985, while in the US such authorisations fall under Title III of the Omnibus Crime Control and Safe Streets Act 1968[3].

6.1.1. DNR-Based Hardwired Taps.

The authorised CI request is presented to a designated employee of a local exchange carrier, who is then mandated to provide administrative and technical assistance to the requesting officers. If the request involves simply the acquisition of 'call data' –namely numbers dialled by the subject of an investigation during a prescribed period– then one of two things usually occurs: (a) if the request involves the suspect's past telephonic activity, then a printout of the suspect's subscriber records is faxed to the requesting officer[4]; (b) if the request involves the suspect's future telephonic activity, then the requesting officer uses a particular kind of 'pen register'[5] device known as Dialled Number Recorder (DNR) (figure 6.1.1a). When attached to the target subscriber's telephone line, a DNR captures all electronic impulses transmitted through the line, including impulses transmitted while in telephonic contact with another party (Freeh 2000). Phrased differently, while in operation, a DNR collects all of the contact numbers that are dialled by a target subscriber. It also prints lists of the contacted numbers accompanied by monographic symbols that indicate ringing, a busy signal, as well as the beginning time of the placement of a telephone call and the precise time that the called party answers (Yarbrough 1999). Some local law enforcement and all intelligence organisations have DNRs in their possession and often use them in parallel with computer software specifically designed to analyse and scrutinise telephone call patterns of targeted individuals or groups (figure 6.1.1b).

6.1.2. Cross-Connect Box Hardwired Taps.

If the CI request involves access to the actual content of communications, then the telecommunications employee discloses to the requesting officers the particular cross-

[3] This legislation was recently amended by the Electronic Communications Privacy Act 1986.

[4] Often, designated telecommunications employees can be contacted with CI requests through the Internet. See for instance BellSouth's on-line CI facility located at http://contact.bellsouth.com/acc/officer_requesting_trace.asp.

[5] Pen register is an antiquated term. It stems from the manner in which the digits in a telephone number were recorded when telephones used pulse dialling technology, which has since been replaced by touch-tone technology. The term still applies to the recovery and recording of the dialling information that addresses a telephone call to and from an intercept subject.

connect boxes[6] that are located between the target subscriber's telephone apparatus and the telephone company's central switching stations, as well as the binding post –that is, the identification number of the target subscriber's line. Once the requesting officers detect the precise cross-connect box in which they wish to install the wiretap, they notify the local exchange carrier employee, who then allows them to lease one of the free lines available in the cross-connect box's 1,800-pedestal[7] (figure 6.1.2a). With this information readily available, the requesting officers are able to install a wiretap without any further assistance from the telecommunications company. With the help of a pair of alligator clips (figure 6.1.2b), a hardwired connection is established between the target subscriber's line and the leased line. The latter channels all telephonic activity on the target subscriber's line to a designated telephone located on the law enforcement or intelligence organisation's premises. Thus, in essence, if one considers a telephone connection between a subscriber and the network's operating centre as a circuit consisting of a pair of copper wires forming a loop, an extra load[8] is connected to the circuit, in a manner similar to installing an additional telephone appliance into a household's existing telephone line. The only difference is that, in a CI operation, the additional telephone appliance is located at the law enforcement or intelligence organisation's premises (Appendix 5). The additional telephone appliance used by the officers conducting the CI operation is usually an ordinary telephone appliance with its microphone disabled, so that it works only as a listening device, connected to adequate telephone surveillance equipment, such as a telephone recorder (figure 6.1.2c) or even a typical voice recorder mediated through an automatic telephone recording device (figure 6.1.2d)[9].

6.1.3. Loading Coil-Based Hardwired Taps.

Another, though less popular, place to install a wiretap during a CI operation is at the loading coil. Loading coils are induction devices, which are placed by telephone carriers on analogue local loops longer than 5.5 kilometres long, in order to compensate for wire resistance and capacitance, and boost the frequencies carrying voice information. Equipped with loading coil and binding post information provided by telephone

[6] Also known as Serving Area Interfaces.
[7] Each cross-connect box usually provides service to 1,800 customers.
[8] That is, a component powered by the circuit.
[9] Additionally, a 'slave' or 'bypass' device is used to provide electrical isolation between the target line and the eavesdropping apparatus.

company employees, law enforcement or intelligence officers climb the telephone pole and use alligator clips to connect a particular subscriber's line in the loading coil to a radio transmitter, which in turn transmits the required sound data to a recording receiver located within the law enforcement or intelligence department's premises. The radio transmitter is usually sheltered in a leather pouch known as a 'disguise boot' (figure 6.1.3) and attached to the telephone pole or to the telephone lines (Appendix 5).

Wiretaps installed on cross-connect boxes or on loading coils are known as 'hardwired taps' because their implementation requires physical access to a section of the telephone wire that sound signals travel on. Law enforcement and intelligence officers are well accustomed to undertaking such CI operations and the telephone carrier is usually expected to provide only logistical support.

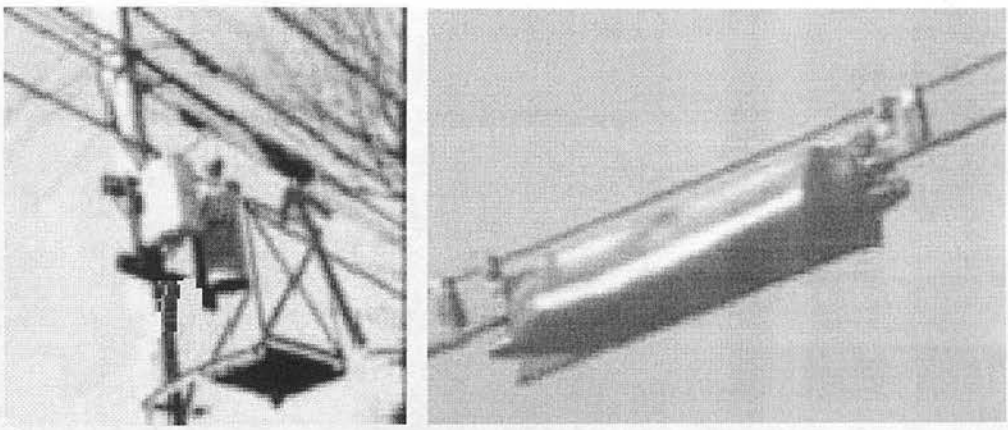


Figure 6.1.3 Example of a wiretap installed at a telephone network loading coil (the large box mounted on the telephone pole). The wiretap, indicated by the grey arrow, is clearly visible in the next picture, which shows the disguise boot containing the radio transmitter (original photographs).

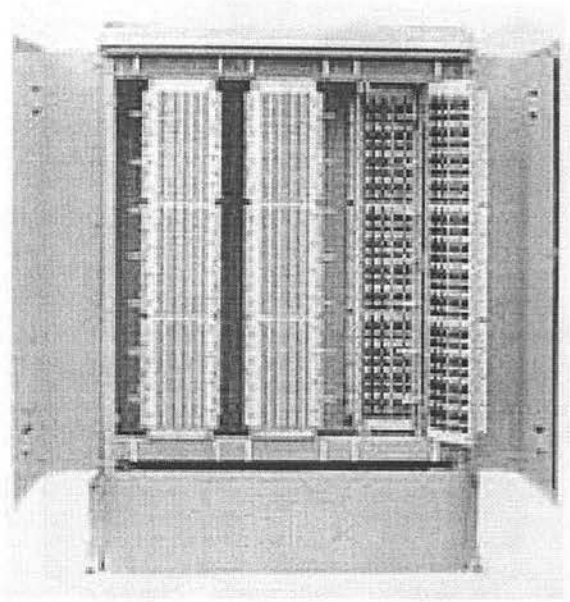
6.1.4. REMOBS Unit-Based Softwired Taps.

A different wiretapping technique, known as 'softwired tapping', was developed soon after the emergence and use of the first mainframe computers for administering extensive telecommunications networks[10]. Softwire tapping requires modification by the carrier's engineers to the software used to run a telephone system. In recent years, softwired taps have become more widely known within the law enforcement and intelligence community as 'translation taps', 'Direct Access Testing Unit (DATU) taps', 'Electronic Switching System (ESS) taps' or, more often, 'Remote Observance (REMOBS) taps'. REMOBS are testing devices used by telephone engineers to run

[10] Softwired tapping has never been acknowledge in the UK, but in the US it emerged during public hearings on telephonic surveillance following the Watergate affair (see USCCGO 1974).

Figure 6.1.1a: This particular DNR, known as Racom 2816D DNR, is used exclusively by government and law enforcement agencies in the US, UK and other countries. It can simultaneously monitor all call activity on up to six target lines. For each intercepted call, Racom 2816D displays and prints a detailed call record (source: Racom Ltd.).

Figure 6.1.1b: A number of DNRs are seen here connected with a designated computer. The marriage between DNRs and especially designed digital software allows the synchronous analysis of electronic call detail records, phone company toll record files, and cellular call records.



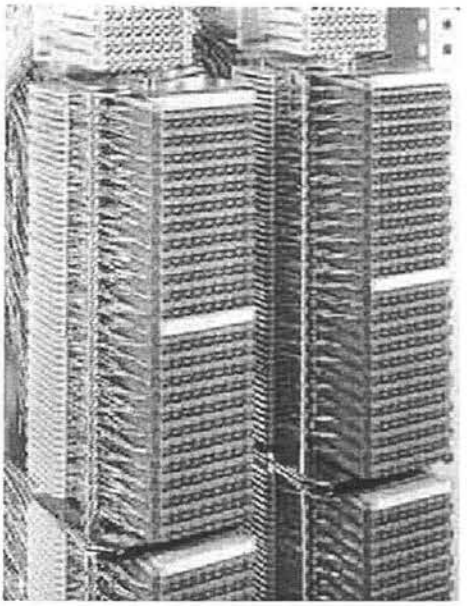


Figure 6.1.2a: Interrior of a typical cross-connection box. Identifying a single cross connection corresponding to a particual subscriber's telephone line would be virtually impossible without assistance from telephone company engineers (original photographs).

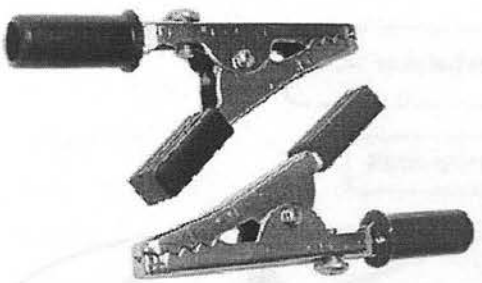


Figure 6.1.2b: Known as 'crocodile clips', these small connection points are used by law enforcement and intelligence officers to establish a hardwire connection between a target subscribers line and a leased line during an interception operation. The clips are used so as to avoid damaging the targeted communications line (source: TechManual, Ltd.).

Figure 6.1.2c: Telephone recorders, such as the P5070 CID pictured here, are used by goverment organisations practicing CI to record the content of telephonic communications. Sophisticated telephone recording appliances are voice-activated and come with built-in dialled number capture and 5-hour recording ability (source: Racom Ltd.).

Figure 6.1.2d: An automatic telephone recoding device, such as the one featured above, can transform an ordinary voice recorder into a voice-activated telephone recorder. Such devices are particularly popular with local law enforcement departments, because they can be up to ten times less expensive than sophisticated telephone recorders (source: TechManual Ltd.).

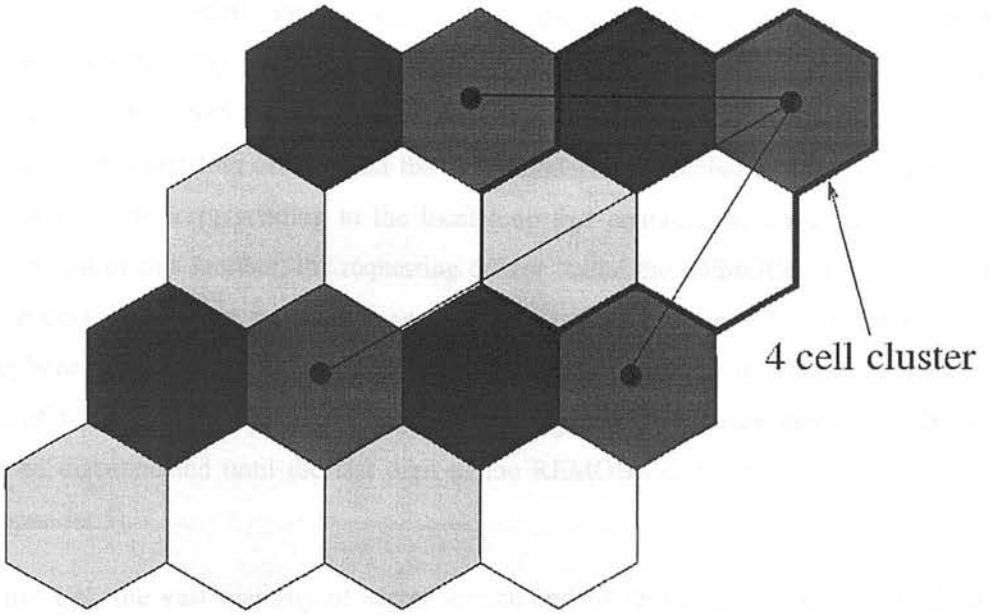


Diagram 6.2.3a: Hexagonal coverage cells form the basis of the cellular telecommunications grid.

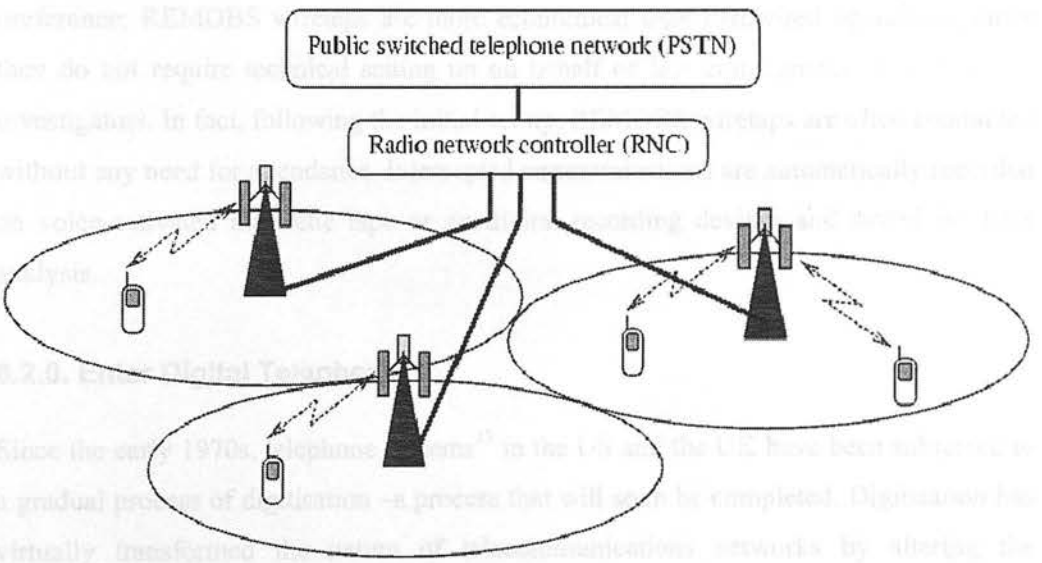


Diagram 6.2.3b: Roaming allows cellular telecommunications users to use a multitude of cell base stations in the course of conducting one telephone call.

frequent tests on local network loops[11]. Through these devices, authorised engineers maintain receive-only access to the content of any customer's line in the telephone system. When served with a valid CI warrant, the local exchange carrier's engineer supplies the requesting officer with the contact telephone number and access code of a REMOBS unit corresponding to the local loop that contains the target line. Once in possession of this number, the requesting officer 'calls' the REMOBS unit and keys in the access code. After the code is accepted, the officer keys in the target subscriber's telephone number and as soon as the last digit of the telephone number is pressed, the officer's telephone appliance becomes permanently connected to the target line and will not be disconnected until the last digit of the REMOBS unit's access code is dialled (Appendix 5).

In the UK, the vast majority of secret service and NCIS CI operations are conducted through REMOBS units, while in the US REMOBS wiretaps are rapidly replacing hardwired CI operations. Financial reasoning is primarily responsible for this change in preference: REMOBS wiretaps are more economical than hardwired operations, since they do not require technical setting up on behalf of law enforcement or intelligence investigators. In fact, following the initial set up, REMOBS wiretaps are often conducted without any need for attendance. Intercepted communications are automatically recorded on voice-activated magnetic tape or on digital recording devices and stored for later analysis.

6.2.0. Enter Digital Telephony.

Since the early 1970s, telephone systems[12] in the US and the UK have been subjected to a gradual process of digitisation –a process that will soon be completed. Digitisation has virtually transformed the nature of telecommunications networks by altering the technical paradigms of communications exchange. Prior to digitisation, telecommunications systems were based on relatively simple networks of copper wires, which carried sound signals by translating them into electrical signals[13]. By contrast,

[11] Each local loop, composed of around 12,000 customer lines is served by a number of REMOBS units.

[12] Including mainframe control and switching apparatuses, as well as transmission techniques.

[13] The addition of electronic amplifiers –to enhance voice signals travelling over long distances– or Frequency Division Multiplexing (FDM) technology –to facilitate higher traffic on the analogue networks– were but trivial technical changes to the basic concept of network telephony that emerged in the late 19th century.

digital technology replaced the language into which sound signals are translated, by substituting electrical signals with binary signals[14]. Thus, in the digital network environment, sound signals undergo a process of transformation from analogue to binary. This process is conducted by a series of electronic circuits, including 'coders'. Coders have the ability to turn on –represented by the digit 1 in the binary system– and off –represented by the digit 0– extremely rapidly, thus translating all sampled sound signals into combinations of 1 and 0. Once the voice signals have been converted into binary format –which occurs at the local carrier's central office– they are carried in digital format though a main trunk into the central office belonging to the local carrier serving the local loop where the message's receiver is to be found. Once there, the signals are processed again, this time by electronic circuits known as 'decoders'[15], which convert the message from binary code back into analogue sound signals. Finally, the signals are carried through the local loop to the telephone handset of the receiver (diagram 6.2.0).

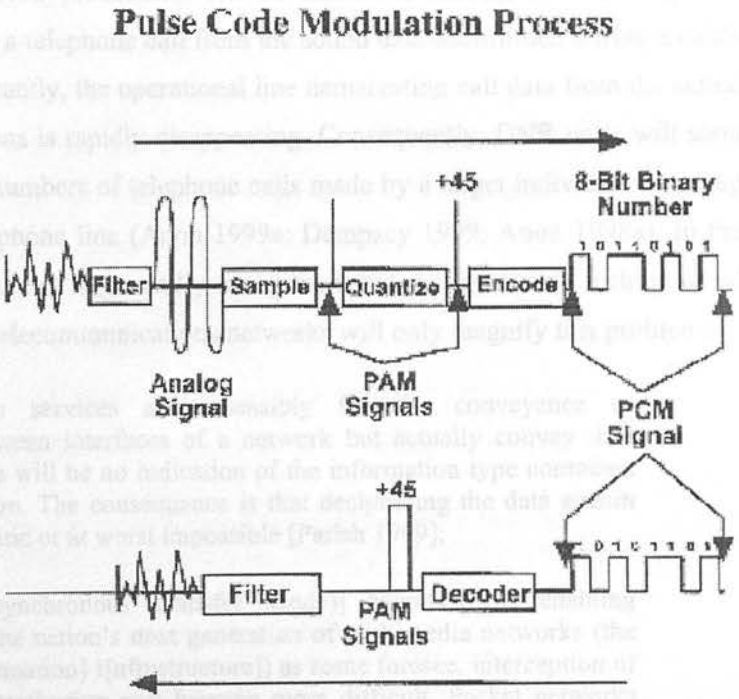


Diagram 6.2.0 In digital telephony, analogue messages are sampled, quantised and coded into binary code, before being forwarded to the carrier's central office. They are then forwarded to the local office of the receiving subscriber's local carrier in digital format.

[14] In the binary code only the digits 0 and 1 are used, since the system uses the base two.
[15] Coders and decoders are usually commonly referred to as CODECs.

6.2.1. Digitisation as a Barrier to CI.

The roots of this procedure, which is known as 'digital encoding', can be traced to competitive economics. Network systems based on binary logic are relatively simple to construct, are reliable, have enormous capacity and –due to advances in the production of silicon circuits– are much cheaper to build and maintain than analogue telephone networks. However, one of the side effects of digital encoding is that it threatens to render traditional hardwired, softwired, and even DNR-based wiretaps virtually useless. Thus it can have a potentially catastrophic effect on law enforcement and intelligence CI operations.

The case of DNR-based wiretapping, arguably the most uncomplicated of CI practices, is indicative of the way in which the digitisation of communications poses structural barriers to even the most basic analogue CI functions. Namely, the automatic conversion of sound signals to binary signals means that, once the telephone network's local loop lines are digitised, network processors will be unable to distinguish the telephone number used to facilitate a telephone call from the sound data transmitted during a call's duration[16]. Phrased differently, the operational line demarcating call data from the actual content of communications is rapidly disappearing. Consequently, DNR units will soon be unable to collect the numbers of telephone calls made by a target individual or group using a fully digital telephone line (Anon 1999a; Dempsey 1999; Anon 1998a). In the relevant technical literature it is generally recognised that the increasing technological sophistication of digital telecommunications networks will only magnify this problem:

> [c]ommunication services are ostensibly for the conveyance of information between interfaces of a network but actually convey data streams, so there will be no indication of the information type contained in the data stream. The consequence is that deciphering the data stream will be problematic or at worst impossible [Parish 1999];
>
> [i]f ATM [(Asynchronous Transfer Mode)] becomes the enabling technology for the nation's next generation of multimedia networks (the N[ational] I[nformation] I[nfrastructure]) as some foresee, interception of electronic communication will become more difficult. Packet networks will require a substantially different approach to surveillance than used for today's digital telephony. Since the address is an integral part of the packet that contains the message data as well, it will be necessary to develop means to insert hooks into the packet header to identify the sender and the intended recipient [Blair, *et al.* 1995].

[16] In the realm of the Internet and voice-over IP, ISDN is a case in point of this blurring of content and communications data. See Appendix 3.

Similar problems have appeared in the other three forms of CI, both hardwired and softwired. The conversion of sound signals to binary signals in a digital network means that, once the local loop is digitised, a hardwired tap installed at the cross-connect box will relay a series of unintelligible sounds[17], rather than a conversation between target subscribers. Even if a wiretap at the cross-connect box were technically feasible –if, say, law enforcement or intelligence officers were in possession of advanced decoders[18] that could instantly translate binary signals back into sound signals– only a small part of the targeted communication would be accessible, due to 'packet switching'. Packet switching is an ATM-based technique through which data streams are fragmented into packets[19] and travel through different routes towards a common destination. Thus, the packetised transmission of a data stream through a digital network can be compared to the journey of a train through a railway network, in which all of the train's carriages are disconnected and allowed to make their way toward the point of destination through different routes, only to be assembled again –in the order in which they began their trip– shortly before arrival. All digital networks, such as the Internet, have evolved as packet-switched networks in order to facilitate constant user demand for faster and more efficient data communication. As large segments of the telephone industry are moving toward an Internet-like model of network communication[20], packet-switch solutions are becoming the norm in voice data exchange. Thus, interception models based on cross-connect box installations are expected to prove increasingly insufficient in meeting the future CI needs of law enforcement and intelligence organisations (Clayton et al. 2000; Dempsey 1999). According to Rodney Small, an FCC employee who handles CALEA issues, packet switching is expected to develop into one of the most corrosive elements in the CI debate between US law enforcement and telecommunications carriers:

> [w]e believe the packet issue is going to be around for a long time [.... Industry has] decided it [i]s too expensive to [facilitate packet-switching-

[17] Similar to those one gets when one listens into a facsimile line.

[18] Meaning Digital-to-Analogue (D/A) converters, such as those used by the carriers themselves.

[19] "A packet is usually defined as the unit of data that leaves one site and traverses the network intact until it reaches the destination site [...]. The packet always contains some network address information to allow the network nodes to route the packet properly to the destination" (Goralski & Kolon 2000). Each packet typically represents a slice of speech lasting 30 milliseconds.

[20] According to some experts, the packetised nature of Internet communications renders every known form of content interception almost practically impossible: "Messages in transit on a backbone IP network are, we believe, difficult to intercept. There is no structure to the flow of data, with many thousands of 'calls' going on simultaneously. Indeed, the way the Internet is operated, with the possibility of alternative routes, means that the packets of data associated with any one transaction do not necessarily follow the same physical path between the end systems" (Smith 1999).

> friendly CI] and they are n[o]t sure what the privacy implications are. They are getting cold feet, legally and financially. Meanwhile, these new technologies keep developing [...]. On the packet data [issue], there could be many petitions and it could be a big mess [ctd in Brown 2001].

Hardwired interception models based on loading coil installations are also disappearing from use, since binary data transmissions do not require amplification from loading coils on lengthy wire routes. The same applies to softwired interception models facilitated through REMOBS units. Most of the quality testing of digital telephony networks is now facilitated through specially designed software running on centralised computer units, and thus REMOBS are rapidly disappearing from use (Yarbrough 1999)[21].

6.2.2. CI and Custom Calling Services.

In addition to the problems posed for CI by changes in the basic structure of wireline telephony, there are a number of additional system features that have been created or enhanced by digitisation, which are already restricting the CI needs of law enforcement and intelligence agencies. These features, which are collectively known as 'custom calling services', include some of digital telephony's most popular consumer preferences, such as call forwarding, speed dialling, three-way calling, automatic recall, and number portability (see chapter 7n23). The particular ways in which such features diminish the CI capacity of law enforcement and intelligence agencies are explained in Appendix 3. It is sufficient to state here that the higher the ability of digital telephony subscribers to control the particular features and capabilities of their telephone service, the lower the ability of an authorised or unauthorised government interceptor to gain access to the call data or call content of subscribers' telephonic communications.

6.2.3. Enter Digital Wireless Telephony.

The digitisation of telecommunications has also had a dramatic effect on mobile communications systems, such as cellular communications and Personal Communications Services (PCS). Such systems have been around for decades and have always posed technical barriers to CI. Nevertheless, their extremely limited functionality and popularity prior to the late 1980s meant that mobile telephones were rarely targeted in state-sponsored CI operations. Digitisation has changed the nature of mobile

[21] See for instance Cisco's IP Telephony Solution Guide, located at http://www.cisco.com/univercd/cc/td/doc/product/voice/ip_tele/solution/index.htm.

communications systems in three main ways: (a) it has reduced the cost of manufacturing mobile telephone handsets; (b) it has reduced the cost of constructing and maintaining mobile communications networks; and (c) it has helped increase the amount of data that can be transmitted through the network[22], which has in turn decreased the costs of communicating through mobile systems. The above three changes were instrumental in facilitating the rapid increase in the use of second-generation cellular communications instruments in the US and the UK throughout the 1990s.

Regardless of whether cellular systems are analogue or digital, they function by dividing an area into small hexagonal cells. Each cell can be sized between 2 and 35 kilometres in diameter and is covered by a base station that consists of a tower and a small building containing the radio equipment necessary for communication. This multiple cell structure allows for extensive frequency reuse across a city or a town, so that millions of customers can use cellular telephones simultaneously (diagram 6.2.3a). More significantly for CI operators, multiple cell structures allow mobile telephone users to roam[23] –i.e. to travel between an area's cells while using the same telephone handset. As a user moves toward the edge of a particular cell, the cell's base station senses the diminishing signal of the user's telephone, while the base station of the cell the user is moving toward, senses the increasingly strong signal of his or her telephone and gradually assumes the necessary reception and transmission functions. Often, the user will roam outside the coverage area of his or her cellular provider, in which case prior industry agreements enable another Mobile Switching Centre (MSC) to assume servicing the user's handset[24].

The mobile nature of cellular telephony means that it is impractical to place a hardwired tap at a particular cell base station, as there is no guarantee that the latter will facilitate all of a suspect's telephone call or calls. Indeed, a particular telephone call may be expected to pass through dozens of cell base stations and a number of different service providers before reaching its destination (diagram 6.2.3b). Additionally, even if a suspect using a cellular telephone is physically immobile, if the particular telephone instrument used is digital, then by the time the suspect's voice signals reach the cell base

---

[22] This is done through digital techniques such as Narrowband Advanced Mobile Phone Service (NAMPS) in the US and Global System for Mobile Communications (GSMC) in the UK.

[23] The term 'intrasystem roaming' generally applies when a user initiates or receives a telephone call in a cell territory other than his or her home area.

[24] In such cases, billing information is automatically exchanged between the original service provider's Home Location Register (HLR) and the Visited Location Register (VLR).

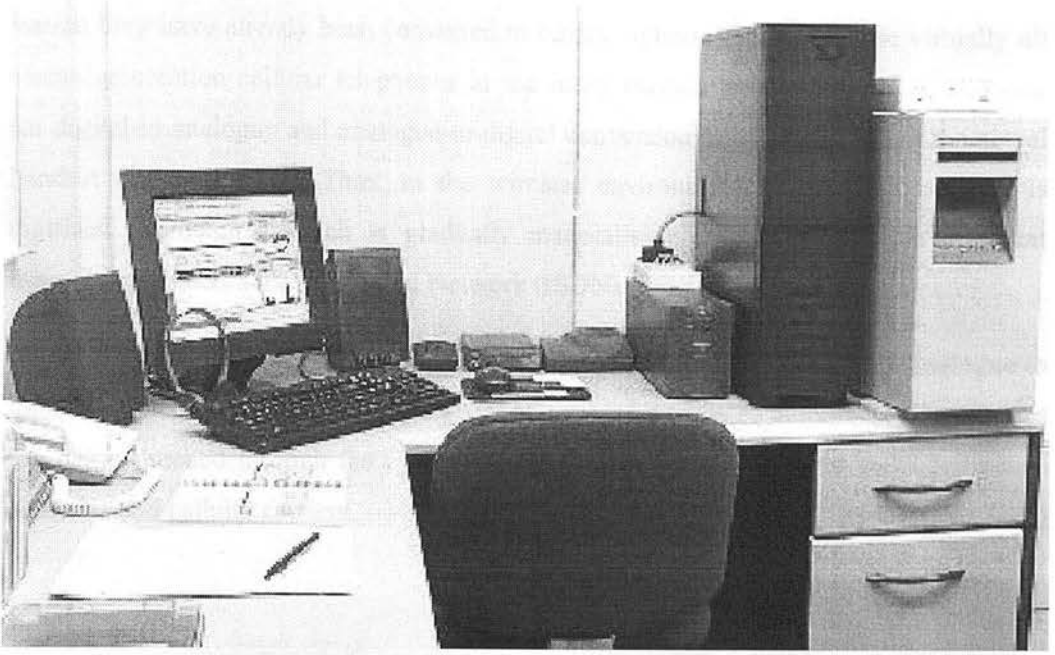


Figure 6.3.1a: The above picture shows a state-of-the-art digital collection unit. The large white box on the right is a Magneto Optical jukebox, a content-storage appliance that records and stores intercepted telephone content data. Storage appliances such as these can hold up to 16 removable discs, each with a storage capacity of 180 hours of uncompressed audio. The large black box next to it is a collection server, which receives intercepted call data and content (original photograph).

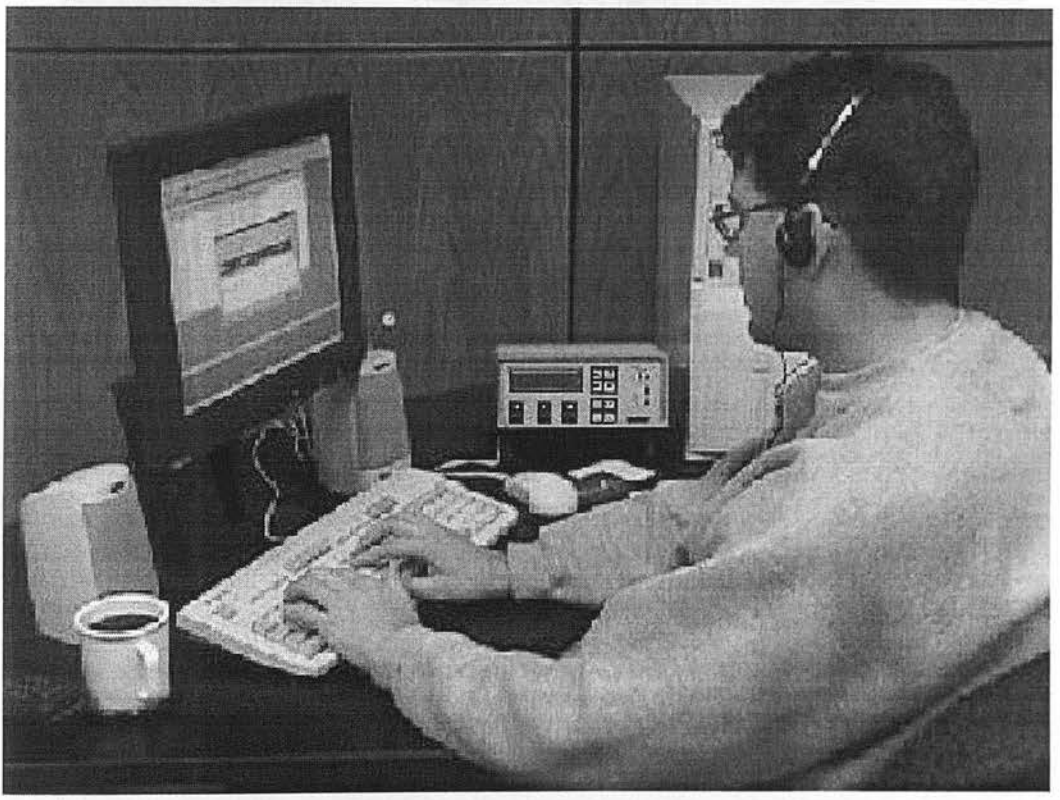


Figure 6.3.1b: This picture shows a state-of-the-art digital collection unit in use. In between the computer screen and the hard drive a DNR unit, connected to the digital collection unit, is visible (original photograph)..

station they have already been converted to binary signals. This is because virtually all second-generation cellular telephones in use today contain built-in CODECs, allowing for digital-to-analogue and analogue-to-digital conversion to be performed at the actual handset (figure 6.2.3)[25]. Thus, in the wireless environment, even the local loop is digitised –something which is gradually materialising in the wireline environment through Integrated Services Digital Network (ISDN).

As an increasing number of cellular telephony providers are switching from analogue to digital, barriers to CI are multiplying and alternative models of authorised CI practices are being pursued through the close co-operation of law enforcement and intelligence agencies and cellular carriers.

Figure 6.2.3 The interior of a cellular phone handset contains a sophisticated computer system. The CODECs, which convert sound signals to binary signals and vice-versa, are contained within the microprocessor. The microprocessor is the large square located at the bottom half of the inside panel –see insert (source Nokia Ltd.).

[25] What this has meant for CI in practice is that it often takes law enforcement or intelligence officers "weeks rather than minutes to decode the conversations" they intercept (Lloyd 1993).

6.3.0. Battling Out for Standards.

Both RIPA and CALEA aim to counter the emergence of digital barriers to CI by demanding that telecommunications carriers provide law enforcement and intelligence agencies with access to communications data and content regardless of its nature[26]. None of the two Acts, however, specifies the precise technical features of this accessibility. Rather, in both cases, the process of deliberating on the technical standards of digital CI has followed the enactment of the legislation[27]. Consequently, in the absence of concrete technical standards, large segments of the two Acts have yet to be enforced. What is more, ever since the enactment of RIPA and CALEA, the quest for acceptable technical standards has emerged as the most contested issue in the digital CI debate. Observers in both the UK and the US remark that, although telecommunications carriers are aware that they are required to provide government agencies with access to digital communications data and content, they are simply in the dark about precisely how this access is going to be facilitated:

> [o]f particular interest to suppliers of communications systems and networks is the technical means by which an interceptor will require to access a user's data stream. Will a system feature with very secure access be required? Are there service and interface descriptions? As currently drafted, the present proposals are too vague [Parish 1999];

> nobody really knows how to do this. I mean, there isn't a blueprint, which has been worked out –at least not [...] one that is known about in the industry– of how this is supposed to happen [Bowden 2000:665-667; see also Int08:184ff];

> [t]he [government] said [CALEA] required us to [...] put certain features into the technology and we said no, the law does not require those features. That was based upon a pushback on cost reimbursement grounds, as well as privacy grounds and [...], frankly, that issue is still open [CALEA Compliance Attorney, BellSouth USA, Int20:85-88];

> it's just sort of this vicious cycle so that [...], even if a company wants to buy equipment [...] and become CALEA-capable or CALEA-compliant, they couldn't because there is nothing out there, because all the manufacturers are waiting to see what is going to happen [Government Relations Director of a large national telecommunications association, Int18:84-92].

In the UK, the technical features of RIPA are still largely unformed. As this thesis is

[26] See CALEA (Public Law 104-414) Section 103(a) and RIPA 2000 Part I(12).
[27] See CALEA (Public Law 104-414) Section 106 and RIPA 2000 Part IV(62).

being finalised for submission, the Home Office is conducting a "detailed technical consultation exercise with CSPs regarding the interception of new telecommunications technologies" (Home Office 2001b), the results of which are not expected to be published before the end of September 2001. Additionally, a Technical Advisory Board will be created under Section 13 of the RIPA, which will, among other things, consider the technical consequences of RIPA's CI capability demands (Home Office 2001a). It is expected that the Board, which will consist of six telecommunications industry representatives and six members of UK law enforcement and intelligence organisations, will be consulted before the British Secretary of State issues secondary legislation defining RIPA's precise technical features[28]. The draft order providing for the membership of the Technical Advisory Board has yet to be put before Parliament and thus the establishment of the Board is not expected to take place before 2002. It follows that observers without appropriate security clearances will not be able to form a lucid picture about RIPA's technical features before well into 2002.

One part of the picture that is already apparent is that the British government is instrumental in determining the specifics of RIPA's technical standards. The very fact that half the members of the proposed Technical Advisory Board are to be drawn from government agencies, places the British government in a position far superior to that of the US government in relation to CALEA's technical standards. Specifically, Section 107 (a)(2) of CALEA contains what is often called a 'safe harbour' provision, which states that

> [a] telecommunications carrier shall be found to be in compliance with the assistance capability requirements under section 103, and a manufacturer of telecommunications transmission or switching equipment or a provider of telecommunications support services shall be found to be in compliance with section 106 if the carrier, manufacturer, or support service provider is in compliance with publicly available technical requirements or standards *adopted by an industry association or standard-setting organisation*, or by the [Federal Communications] Commission under subsection (b), to meet the requirements of section 103 [Public Law 104-414, Section 107 (a)(2); emphasis added].

Phrased differently, the above quote means two things: (a) that, strictly speaking, there does not necessarily have to be a digital CI standard as long as each and every carrier is

[28] There is uncertainty as to the degree of transparency that will characterise the Technical Advisory Board. It has already been agreed that its members should be security-cleared, that its meetings should be held in confidence and that it should report directly to the Secretary of State (Home Office 2001a).

willing and able to comply with CALEA in any way they see fit[29]; and (b) that if technical standards are to emerge, they have to do so out of an industry consensus. Hence, law enforcement and intelligence agencies are not permitted to impose their own CI standards on the industry[30]. The safe harbour provision was not present in CALEA's early drafts; rather it was the outcome of intense and well-calculated industry and civil liberties lobbying efforts aiming to ensure that, as one USTA lobbyist put it "law enforcement can't take us" (USTA CALEA lobbyist and point person, Int16:239):

> according to the law [that] was enacted [law enforcement] cannot dictate to the switch manufacturers how to design the [CALEA-compliant] solution and they cannot dictate to [...] the carriers [...] how to provide delivery to them. They tried [...]. I mean, they [...] would love to. They even made 'suggestions' on how they would like to have it. But when [...] we make a decision, our decision is based on the best interest of [our company] [CALEA Project Manager of a large US telecommunications carrier, Int21:29-34; see also Int18:47-51; Anon 1997a; United States Court of Appeals 2000].

The safe harbour provision allowed the industry to generate and adopt an interim technical standard known as J-STD-025 (USTIA & USEIA 1997), which the law enforcement and intelligence community has described as "wilfully deficient in providing law enforcement the technical capabilities it needs" (FBI Special Agent, Int19:104-104) and has rejected it as inadequate to protect public safety and national security. This confrontation resulted in a rupture in relations between the industry and the law enforcement and intelligence community, which led to several lawsuits and serious delays in the implementation of CALEA. Consequently, as this thesis is being finalised for submission, large parts of digital CI standards are still undecided, more than seven years following the enactment of CALEA[31].

---

[29] "[T]he law also says that you really don't need a standard, as long as you can [...] comply [with CALEA]. But then that means everybody is doing it differently and it becomes a mess. So, both manufacturing and the industry would like to see definitive standards" (USTA CALEA lobbyist and point person, Int16:249-251).

[30] "Law enforcement [...] can't dictate how they have that [policing] presence [on the networks]. CALEA does [...] give the government the opportunity to [...] demand that our technology, as we change it, allows them to continue to conduct electronic surveillance; but they cannot tell us how to do that. It's a very [...] fine distinction, but it's very much present in the law" (CALEA Compliance Attorney, BellSouth USA, Int20:47-49; 60-65).

[31] US Carriers have often accused the FBI of delaying the construction of data collection systems, which means that "even if a carrier were poised to install CALEA-compliant equipment, there would be no means for testing the equipment or even for law enforcement to receive any information once the equipment is installed" (Baker et al. 1998).

6.3.1. The Switch Solution.

A basic principle of digital CI that will inevitably guide RIPA and CALEA's technical standards is that, short of being able to install a listening bug on the suspect's telephone handset, the only place in the digital telecommunications system where a wiretap can be successfully installed is at the switching equipment, located at the local exchange carrier's central office (Blair *et al.* 1995)[32]. The switches are complex computer instruments that have replaced the role once held by human operators in the telephone system. All telephone numbers called within the vicinity of a particular local exchange carrier are channelled to the central switches, located at the company offices. Once there, switching software is able to connect the telephone line of the calling party with either the telephone line of the called party –if the latter is located within the same vicinity– or with the central switches of another vicinity –if the called party is located elsewhere. Without central switching equipment, the lines of all the subscribers in a telephone system would have to be interconnected –as was in fact the case in the very early days of telephony. The simplification of the network, which is facilitated by the existence of central switches, arguably renders the latter the most fundamental components –the structural core– of a sophisticated telephone network. It is right at this core that CI will need to be facilitated in the digital environment:

> [law enforcement] realised that these new features and functions required a lot more flexibility [...] to target and that the only one who really knows what's going on is the switch [USTA CALEA lobbyist and point person, Int16:23-29].

In the US, where the quest for CALEA's technical standards is chronologically more advanced than UK's RIPA, the telecommunications industry has proposed that switch-based CI is to be carried through a 'delivery function' and a 'collection function' system (USTIA & USEIA 2000:17ff). Delivery function, namely the intercept port installed on a switch, will consist of two distinct types of channels: a 'call content channel' and a 'call data channel', each intercepting a respective segment of target telephone calls. The intercepted data will be forwarded to the collection function, which is controlled and maintained by the intercepting agency (Electronic Surveillance Task Force 1997). In a CALEA-supporting environment, the call collection function is less likely to be a DNR

[32] Also known as the 'telephone exchange'.

unit or a telephone recorder and more likely to be a high-speed personal computer (figures 6.3.1a; 6.3.1b) operating on specially designed interception software (figures 6.3.1c; 6.3.1d; 6.3.1e). The same delivery and collection functions will be implemented in the cellular telecommunications environment, with call content and call data delivery channels applied to the MSCs of cellular carriers (USTIA & USEIA 2000:83ff).

This change in the physical location of the wiretap is more significant than it may initially appear. This is because it implies three fundamental changes to the technology and practice of CI:

(a) under the present state of technology, it is not possible to establish a hardwired tapping connection to the central switch without causing a breakdown to the switch's programmable functions. Instead, the order for a wiretap has to be given through the computer software that monitors the performance of the switch. Since the monitoring computers are located within the carrier's central offices, it is designated carrier employees who have to install the wiretap pertaining to a CI request. Therefore, in essence, the traditional role of the carrier in CI operations is revolutionised, as the latter assumes not only logistical but also operational responsibilities under the new regime;

(b) as a direct result of the carrier's augmented role in CI, the role of law enforcement and intelligence personnel in CI operations is likely to be heavily compromised. Under the new regime, the latter will have virtually no input in, or control over, the technical installation of a wiretap. Instead, a leased line provided by the local exchange carrier will provide them with the required telephone call data or content[33].

(c) digital central switches have not been designed with interception in mind (Int04:272-275; Int17:12-22). Thus the industry's standard blueprint for central switching mechanisms will have to be altered to reflect RIPA and CALEA's recommendations. Namely RIPA and CALEA-compliant switches will have to be designed with an additional port that will allow for the parallel feed of intercepted data (see chapter seven,

[33] In the UK, this structural change in CI operations has been observed since the mid-1990s: "[t]he introduction of digital switching in the telephone system has changed the method of telephone-tapping by British Telecom (BT) which it provides on an agency basis to MI5, Customs, Special Branch, the National Criminal Intelligence Service, and police forces. Under the old 'Tinkerbell' system, tapping circuits had to be physically connected to targeted phone lines. Now 'taps' are simply set up using the software programs within the exchange switching system, moreover this is done remotely without ever going near the telephone exchange building. The 'requesting agencies' increasingly have intercepted calls relayed directly to their headquarters where they can analyse and transcribe telephone calls" (Fitzgerald 1994:30).

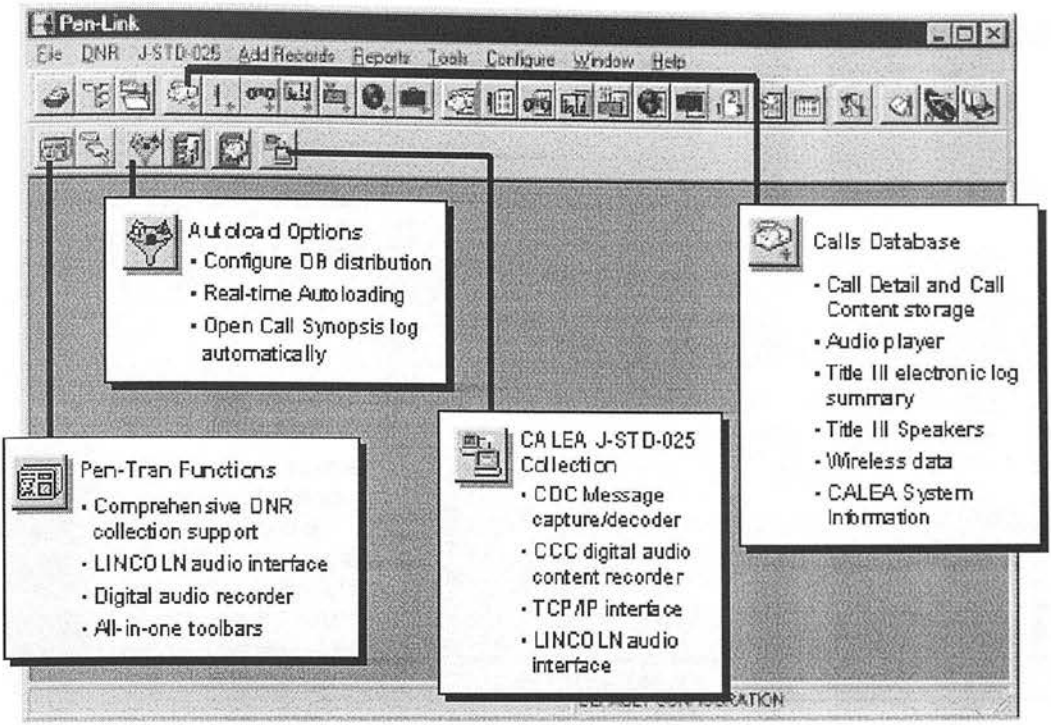


Figure 6.3.1c: One of the more popular CI software among law enforcement and intelligence agencies is Pen-Link's Lincoln. Lincoln is designed to work in the MS Windows environment. Its main interface window is shown here (version 7.0) and some of its main functions are described (source Pen-Link Ltd.).

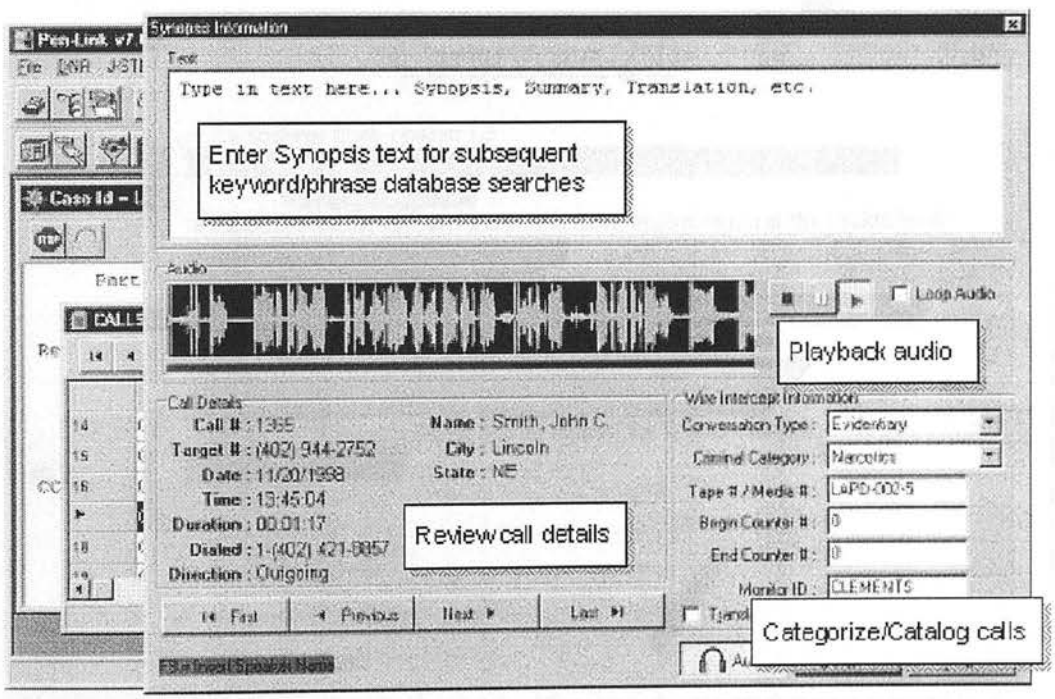


Figure 6.3.1d: Pen-Link's interception monitor interface at work. This software digitally records audio call content from a wiretap, in real time, using industry standard digital .wav encoding algorithms. Audio is routed automatically to authorised monitors. Recordings are automatically loaded into databases, along with corresponding call detail data, for playback and analysis (source: Pen-Link Ltd.)..

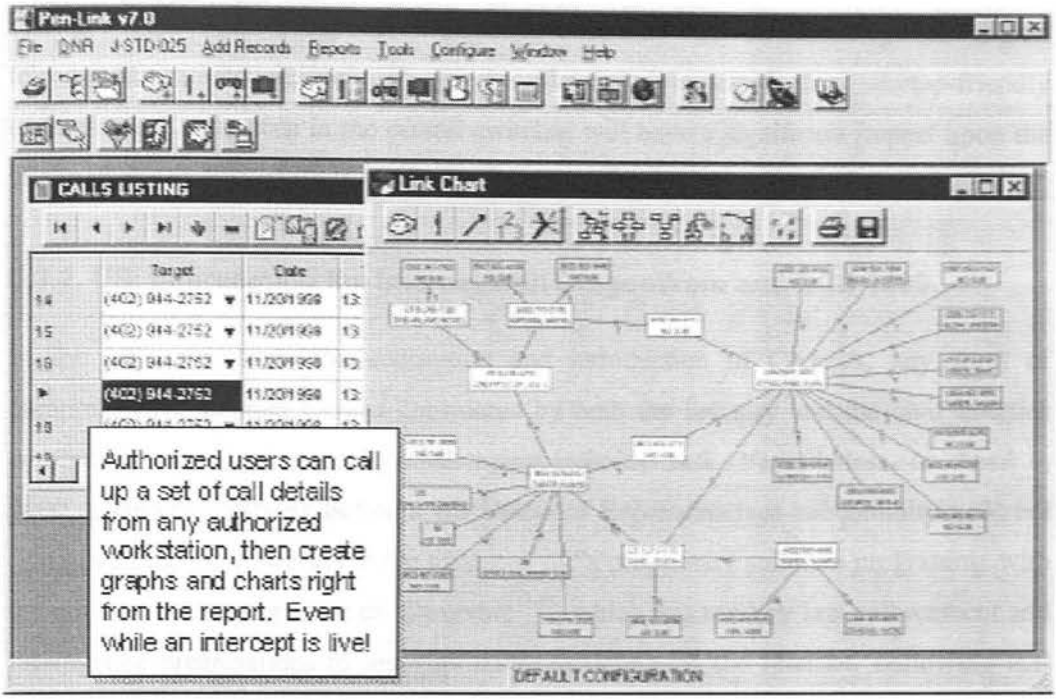


Figure 6.3.1e: Sophisticated CI software has the ability to create instant visualisations of call data patterns of target individuals or groups.

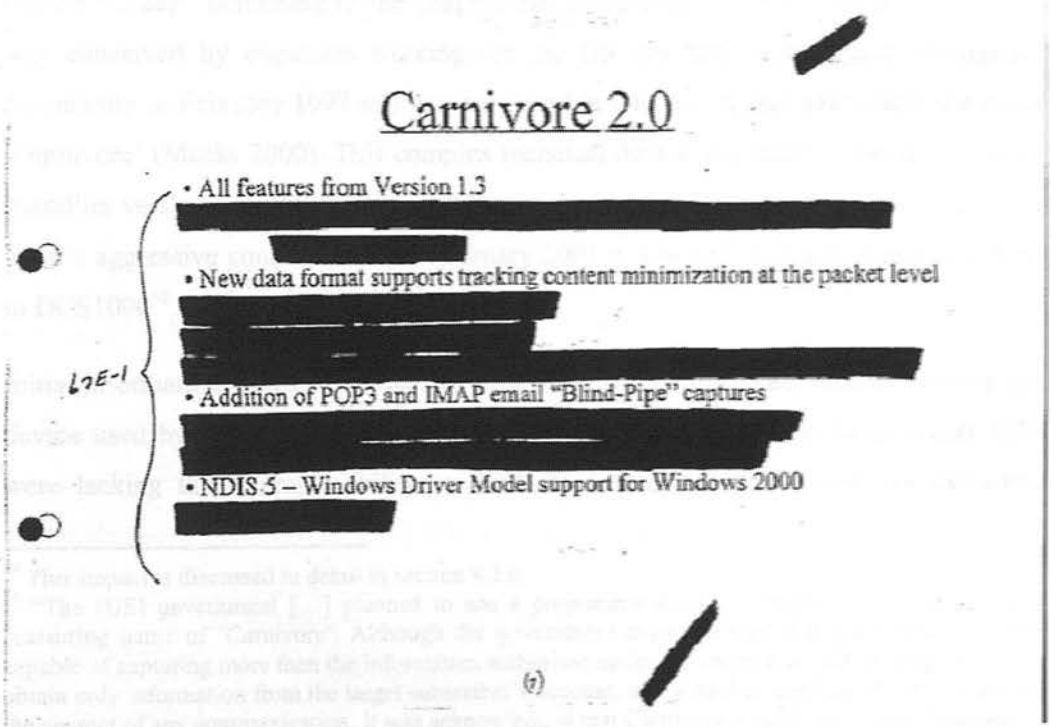


Figure 6.3.2a: A typical page from the first batch of Carnivore documents that were released by the FBI in the summer of 2000 (source: Centre for Democracy and Technology).

section 5.4). Considering the functional centrality of switches in the digital telecommunications network, it can be plausibly suggested that wiretap-friendly technological alterations in the central switches will have a significant impact upon the very nature of telephony in the digital environment[34].

6.3.2. US: Intercepting the Internet with DragonWare and DCS 1000.

In the US, ever since the conception and introduction of CALEA, any form of comprehensive Internet CI was considered by both the industry and the civil liberties community as an exceptionally challenging technical task. Nevertheless, on April 6, 2000, a lawyer testifying before a US House of Representatives subcommittee alerted non-governmental observers to the existence of "a proprietary software programme with the not very reassuring name of 'Carnivore'"[35], which was used by law enforcement and intelligence organisations to intercept data circulating on the Internet. Following that initial revelation, and under legal pressure from FOIA applications filed by civil liberties organisations, the FBI released a number of heavily edited and abridged documents (figure 6.3.2a)[36] pertaining to the programme. According to the documents, Carnivore was conceived by engineers working for the US law enforcement and intelligence community in February 1997 and was first used in October of that year under the name 'Omnivore' (Meeks 2000). This complex technical device was then replaced by a user-friendlier version[37], which was named Carnivore and –following heavy criticism over the word's aggressive connotations– in February 2001 it was once again renamed, this time to DCS1000[38].

Initial information provided by the FBI said that DCS 1000 was an Internet interception device used by the law enforcement and intelligence community in cases where ISPs were lacking the technical ability to facilitate authorised CI requests. As explained

[34] This impact is discussed in detail in section 8.3.0.

[35] "The [US] government [...] planned to use a proprietary software program with the not very reassuring name of 'Carnivore'. Although the government acknowledged that Carnivore would be capable of capturing more than the information authorised under the order, it would be programmed to obtain only information from the target subscriber's account, and would be configured not to intercept the content of any communication. It was acknowledged that Carnivore would enable remote access to the ISP's network and would be under the exclusive control of government agents" (Corn-Revere 2000).

[36] When the FBI released the first documents on Carnivore, in October 2000, more than half of the 750 pages offered to the public were blacked out and hundreds more were withheld (Lemos 2000).

[37] Reportedly running on Windows NT-based computer systems.

[38] DCS stands for Digital Collection System.

above, in section 6.2.1, packetisation of digital communications constitutes one of the primary barriers to intercepting digital messages. Consequently, as the number of CI requests issued to ISPs by governmental intercepting agencies increased over the years, so did the number of cases where ISPs were unable to decode packetised data. This phenomenon triggered the creation and use of DCS 1000[39]. Thus, the technical novelty of DCS 1000 is not that it is able to intercept packetised data, but rather that it is able to decode the information contained in them and distinguish between data referring to call-identifying information and to call content[40].

Initially, non-governmental observers were under the impression that Carnivore was a email surveillance technology, which was able to intercept information pertaining either to the sender and receiver addresses of an email message or to the actual content of the email –depending on the level of authorisation permitted by the interception warrant. A few months later, however, once further technical documents were released under the FOIA, it became clear that Carnivore is a mode of function of a larger Internet surveillance instrument known as 'DragonWare Suite'. DragonWare consists of three software programs: (a) Carnivore, which collects email data and content (figure 6.3.2.b); (b) 'Coolminer', which collects Internet pen register data (figure 6.3.2c); and (c) 'Packeteer', which uses data collected by both Carnivore and Coolminer to reconstruct web sites exactly as they were when a target Internet surfer accessed them (Meeks 2000).

The FBI, which is thus far the only US government agency to have admitted to possessing DragonWare technology[41], has thus far refused to reveal its source code and technical specifications. But it has acknowledged that Carnivore –DragonWare's primary interface with the network– is a by-product of commercially available monitoring tools, which ISP network administrators use for network oversight and management[42]. Virtually no information has been disclosed about the technical features of the hardware that is connected to the network and collects the intercepted data.

---

[39] "In recent years, the FBI has encountered an increasing number of criminal investigations in which the criminal subjects use the Internet to communicate with each other or to communicate with their victims. Because many [...] ISP[s] lacked the ability to discriminate communications to identify a particular subject's messages to the exclusion of all others, the FBI designed and developed a diagnostic tool, called Carnivore" (Kerr 2000).

[40] "Carnivore has the ability to separate content and call identifying information. That's what Carnivore is about" (Michael Warren, Senior Project Manager, FBI CALEA Implementation Section, ctd in Cisneros 2000).

[41] The Bureau has admitted to possessing approximately 20 Carnivore boxes, which are stored in its Quantico, VA, headquarters.

[42] Such as, for instance, EtherPeek, or the Ethereal freeware.

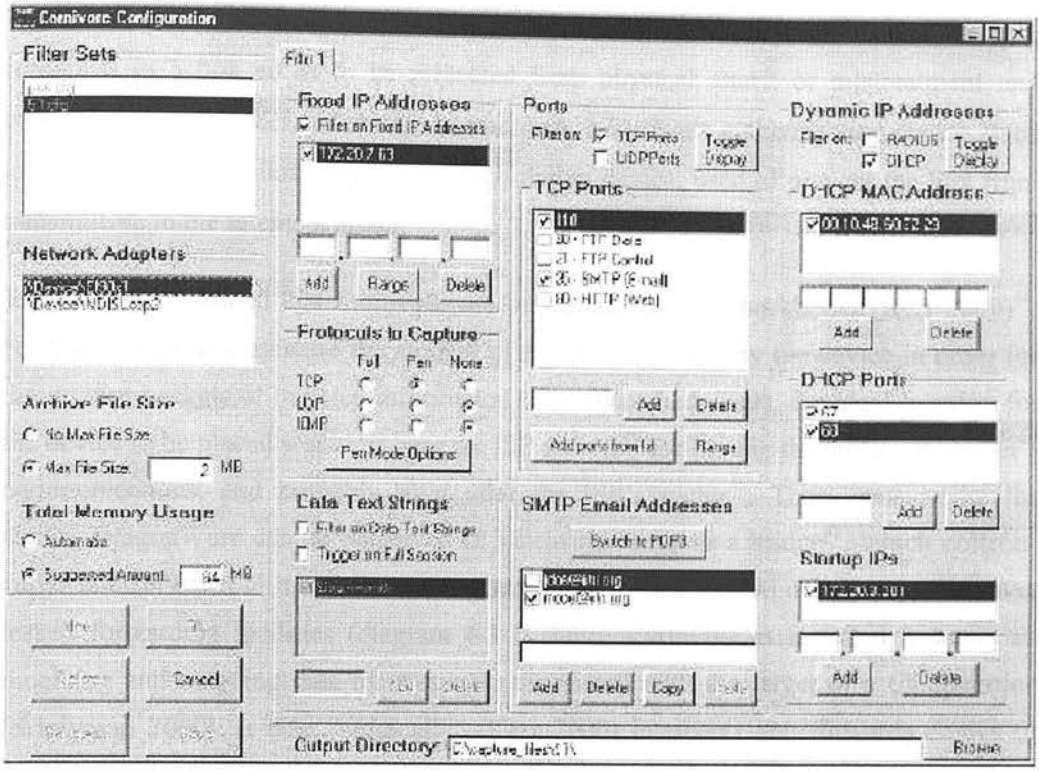


Figure 6.3.2b: Carnivore's configuration interface, which is based on Windows NT technology (source Centre for Democracy and Technology).

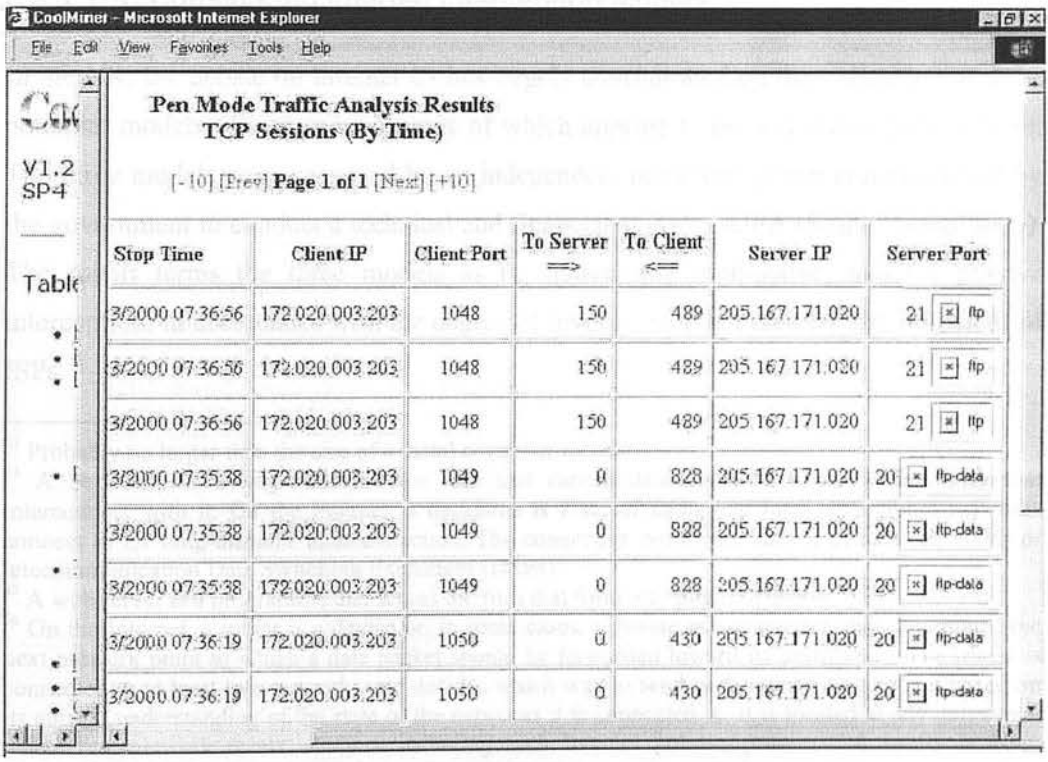


Figure 6.3.2c: Coolminer's main interface. Coolminer collects pen register data of a target IP number's Internet activity (Center for Democracy and Technology).

Nevertheless, it can be safely inferred that the device is small enough to be portable[43], contained in a box so as to be protected from physical attack or mistreatment and containing, among other switch-like components, a hardware authentication device, used to control-access the box, and a network isolation device, used to prevent the box from transmitting to the intercept target.

The FBI has indicated that Carnivore can be installed on ISP backbones (Kerr 2000)[44], but that would only increase the amount of data to be filtered by the device in order for the precise packets of targeted information to be identified. Thus, the ideal location for the device to be placed would be near the ISP servers[45] facilitating the target subscriber's communications, and probably right after the ISP's router[46]. Thus, considering the above, DragonWare can be perceived in schematic terms as a bridge[47], which collects, copys and forwards all traffic from a subscriber's line to a central collection point, over leased forwarding facilities (diagram 6.3.2). Once Carnivore is installed it scans all incoming and outgoing data for messages associated with the target of a CI operation (Srinivasan 2000). It then "surgically" (Kerr 2000) intercepts and forwards copies of these messages to the intercepting officers.

6.3.3. UK: Considering Internet Interception Models.

In the UK, the debate on Internet CI has largely concentrated on the evaluation of three potential models of interception, none of which appears to be replicating DragonWare. The three models were proposed by an independent marketing group commissioned by the government to conduct a technical and financial study of RIPA (Smith Group 2000). The report terms the three models as (a) active; (b) semi-active; and (c) passive interception, in accordance with the degree of involvement that they require on behalf of ISPs.

---

[43] Probably no larger than the size of a metal computer cabinet.

[44] A backbone is a large transmission line that carries data gathered from smaller lines that interconnect with it. On the Internet, a backbone is a set of paths that local or regional networks connect to for long-distance interconnection. The connection points are known as network nodes or telecommunication Data Switching Exchanges (DSEs).

[45] A web server is a programme that serves the files that form web pages to users.

[46] On the Internet, a router is a device or, in some cases, software in a computer, that determines the next network point to which a data packet should be forwarded toward its destination. The router is connected to at least two networks and decides which way to send each information packet based on its current understanding of the state of the networks it is connected to. It is located at any gateway – where one network meets another– including each Internet point-of-presence. A router is often included as part of a network switch.

[47] In telecommunication networks, a bridge is a product that connects a local area network to another local area network that uses the same protocol.

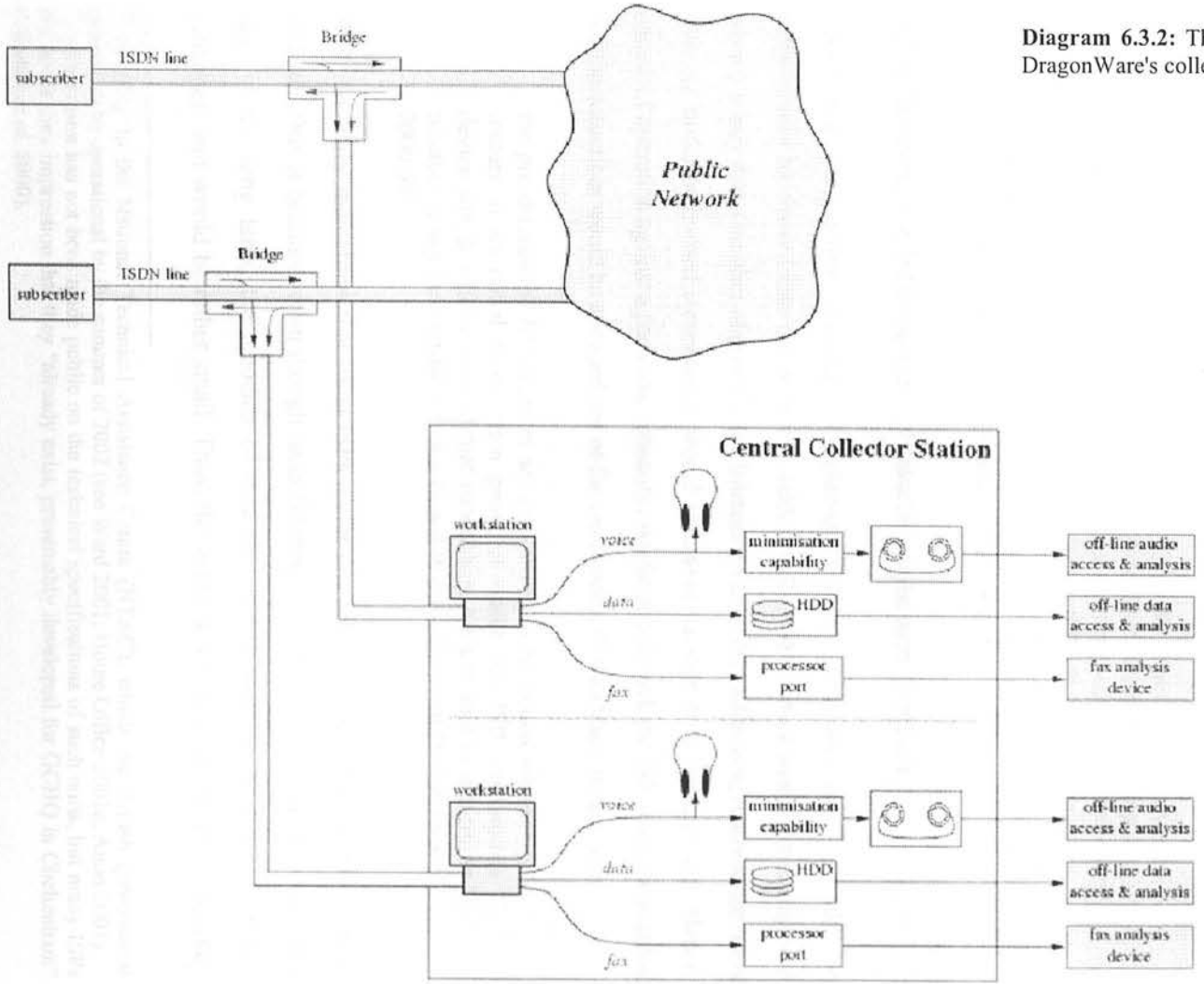


Diagram 6.3.2: This diagram shows the main functions of DragonWare's collection, delivery and analysis components.

6.3.4. Active Interception of Emails.

Under the active interception scheme –applicable only to email surveillance– a software-based wiretap would be configured by authorised ISP personnel at the ISP's email server. Targeted incoming and outgoing mails would then be automatically copied and forwarded by the server to a "government host"[48] (ibid.:38), which could be as rudimentary as a government email address (ibid.). This suggestion will probably be adopted by the British government, as it is technically efficient and it appears to be causing little displeasure among the industry:

> [i]f the interception aim is modest, just to read the target's email, then the task may be simple. Even with permanent connections and certainly with dial-up accounts, the ISP will be running a store-and-forward system for email. Making a copy of the email as it passes through the ISP system is straightforward –you just need a configuration file that says this is to be done. Such a file can be trivially created by any administrator when served with a suitable warrant [Brown *et al.* 2000:7].

6.3.5. Semi-Active Interception of Internet Data and Content.

Under the semi-active interception scheme, a data collection unit[49] would be permanently hardwired into the network. Additionally, ISP routers would be configured in such a way that a number of pre-selected Internet Protocol (IP) addresses, reserved for users who are under authorised surveillance, would be routed through the collection unit. Hence, once a CI operation against a particular subscriber would be initiated, the ISP would be notified and the subscriber would be assigned one of the pre-selected IP addresses. In this way,

> the pre-determined IP addresses are guaranteed to be routed via specific routers at an initial interception point, at which the ISP interception device sits. It will be ensured that subscribers are not able to determine whether or not their traffic is being forced to pass this point [Smith Group 2000:39].

There are early indications that some ISPs prefer this scheme to the passive interception scheme. This is because, even though reconfiguring the network's routers is a complex task, in the long term, the amounts of data that would have to be filtered by the collection unit would be rather small. Thus, the network's overall speed and efficiency

[48] Possibly to the National Technical Assistance Centre (NTAC), which the British government expects to be operational by the summer of 2002 (see Ward 2001; Home Office 2001c; Anon 2001).
[49] Information has not been made public on the technical specifications of such units, but many ISPs are under they impression that they "already exist, presumably developed for GCHQ in Cheltenham" (Clayton *et al.* 2000).

would not be threatened (Clayton *et al.* 2000).

6.3.6. Passive Interception of Internet Data and Content.

Similarly to the semi-active interception scheme, the passive interception scheme also requires a data collection unit to be permanently hardwired into the network. The difference is that, under the passive scheme, the unit would continuously mediate all Internet traffic that passes through the network. While allowing data sent or received by non-target users to pass through without being tampered with, it would automatically copy and forward to a predetermined location all data sent from target subscribers. Under this scheme, government agencies would be in charge of providing, installing and maintaining all hardware and software components of the interception system and would also implement CI operations against users without having to inform ISPs of these users' IPs or names (Smith Group 2000:37).

6.4.0. Towards a Permanent Interception Presence.

A particularly significant variation between the already practised or proposed UK and US Internet interception schemes under CALEA and RIPA concerns the uneven degree of permanence that characterises them. Namely, in the US, DragonWare and its interception point, Carnivore, are not permanent features of the telecommunications network, but are rather deployed and installed to facilitate ephemeral CI operations. By contrast, both the semi-active and the passive interception models proposed in the UK under RIPA have their basis on a conception of interception units as integral components of public telecommunication networks. Independent observers have criticised such plans, insisting that

> [i]n practical terms, this requires the development of black boxes, installed at each ISP, that will send traffic data to the [National] Technical Assistance Centre, located within the Security Services [Brown *et al.* 2000:5].

The British government's plans are often compared to the implementation of Russian Internet interception system SORM-2[50], under which all of the nation's ISPs are legally bound to install an interception unit permanently linking them to the Russian Federal Security Service (FSB):

[50] Translated, SORM stands for System for Operational Investigative Activities (see List of Abbreviations Used).

> The similarity with the UK is already striking. RIP will mandate black boxes at all ISPs. [We are] following the path set by Russia when it comes to interception almost exactly [ibid.:33].

6.5.0. Summary.

There was a time when state-sponsored CI was plain and simple. That time was brought to an abrupt end by the telecommunication industry's pursuit of digitisation. The latter was seen as injecting unmatched dynamism to the newly denationalised market, but it severely compromised the CI needs of law enforcement and intelligence organisations. This compromise, which threatens to drive these organisations out of business, eventually led to the emergence of RIPA and CALEA. Under these new regimes, the structure of CI will change dramatically, marginalising the role of government agents and centralising the role of the carriers in the implementation, oversight and maintenance of wiretaps. In addition, certain elements in digital CI models will require the redesign of structural components of the digital telecommunications network, so as to render it interception-friendly. This applies not only to the telephone network, but also to the Internet, where new government-sponsored technologies are gradually overcoming the network's design barriers against CI.

Chapter Seven
Elements in the Digital Interception Debate

7.0.0. Introduction

This chapter presents the findings of the interviews conducted in the course of this project. Material collected from other primary and secondary sources is also exhibited in an attempt to outline vital elements in the contemporary digital CI debate currently unfolding in the UK and the US.

7.1.0. Interception of Communications as a Social Tool.

There is a lengthy historical tendency within the law enforcement establishment in the UK and the US to regard CI as a fundamental pillar of investigative competence. Undoubtedly, intelligence organisations have traditionally been much more familiarised with the ideology and culture of CI than strictly police organisations. This is because of the sheer volume of information that is surreptitiously acquired, processed and analysed by intelligence apparatuses, as opposed to the more public and visible communications role of policing bodies. Nevertheless, the increasing reliance of models of policing on communications and information management, of which CI is part, should not be underestimated. In their groundbreaking ethnographic work on the communications practices of Canadian police, Haggerty & Ericson (1997) describe the role of policing in a risk society as one of brokering to large administrative institutions and organisations that operate on the basis of risk knowledge. Thus the optimisation of CI practices and

techniques by increasingly organised and bureaucratised law enforcement bodies is a direct consequence of the perceived need by those bodies –and by society at large– to respond to the external demands for risk knowledge, that is, the societal process of accessing and communicating vital information about danger and risk (ibid.:ch1)[1].

In the UK, few, if any, public references are ever made to the extent of usefulness of CI for law enforcement[2]. In the US, however, federal agencies have repeatedly stressed the operational value of CI[3]. FBI Director Louis J. Freeh has remarked that court-ordered CI is

> the single most effective investigative technique used by law enforcement to combat illegal drugs, terrorism, violent crime, espionage and organised crime [Freeh 1995].

Law enforcement interviewees in the US wholeheartedly confirmed Freeh's statements, in responding to the hypothetical question "what would happen if the right of US law enforcement agencies to engage in CI was revoked by Congress?":

> I think I'll be safe in saying that the voice of law enforcement would [...] cry out if there was any revocation of that authority to do intercepts [.... W]e would have a hard time recovering. Law [...] enforcement has depended so much on electronic surveillance –and I'm talking about telephonic intercepts– as a means by which to gain enough evidence to convict people; it has been an incredible tool for us and without it we would be lost when it came to complex investigations [FBI Special Agent, CALEA Implementation Section, Int19:258-262, 275-276][4].

Similar answers by UK law enforcement interviewees further support this perceived interdependency between criminal or intelligence investigations and CI:

> I do not believe law enforcement could carry out its role without the ability of interception. In terms of when to intercept, that is debatable. But the actual facility to be able to intercept I think you have to have it [.... T]he law enforcement agencies have got to have some way to be able to get into those types of organisations and interception is just one of those [Former Special Branch Officer, Int12:6-14].

---

[1] The authors go so far as to assert that the particular features of communications systems, including surveillance systems, actually govern the institutional relations within law enforcement bodies as well as their efficiency and success in relation to their perceived aims (Ericson & Haggerty 1997:4).

[2] "Interception of communications plays a crucial role in helping law enforcement agencies combat criminal activity" (White 1999).

[3] "Without that capability and coverage, we would be out of the counterterrorism and counterintelligence business, as far as I am concerned" FBI Director Louis Freeh (1997a); see also Freeh's statements in 1997b.

[4] See also Int14:33-36: "I've never even thought how hard it'd be to [...] infiltrate a group of criminal or espionage agents without the ability to intercept their private communications [...]. It's the 'A' of our intelligence-gathering alphabet [...]".

This interdependency is not seen as inevitable; rather, it is imposed upon law enforcement agencies by lack of financial resources and the increasing penetration of organised societies by advanced telecommunications systems[5].

Historically, this view of CI as a required element of policing in advanced societies has rarely been questioned by the carriers and providers of electric or electronic communications on either side of the Atlantic. In the US, the telecommunication industry's collective representation bodies are often eager to stress their historical commitment to allowing law enforcement access to their communications networks[6]. A similar outlook permeates the attitude toward communications policing of collective industry representative organisations in the UK (Parish 1999; Emery 1999; Sutter 2001). Indeed, interviews with informed industry representatives in both the US (Int20:112-114; Int21:20-21) and the UK[7] showed that there is little variance of opinion among providers and carriers in regards to law enforcement's right to maintain a structured presence in communications networks. An interesting distinction can be noted in that UK industry officials appear to be motivated to accommodate law enforcement needs by virtue of legal requirement, whereas their US colleagues stressed corporate etiquette and civil duty as sources of their motivation:

> I think traditionally the telecom[munication]s industry have always recognised that they're in a business which is required to provide this sort of service to the authorities in the areas of commerce –whoever these

[5] "[IC] saves them an indefinable amount of resources for the same information. The information they might get from an intercept –from one intercept– might take a surveillance team [or] operation in excess of 12 months; and they might not even get the same information to the same quality and quantity. So, you know [...], if you're looking in terms of resources and cost, the return they are getting in terms of intercept far outweighs the cost, effort and resources they'd have to put in to get that in terms of that information in another way –in the normal, traditional way" (Former Special Branch Officer, Int12:40-46). See also Int14:229-232 "I mean, you haven't always had electronic interception; law enforcement was still able to get results before wiretapping, but back then you didn't have telephonecommunication systems [in] everyday use either" (First Class Sergeant, Communications Officer, United States Special Forces).

[6] "The telecommunications industry has always cooperated, and is committed to continuing to cooperate, with lawful and authorised law enforcement electronic surveillance activity" (Anon 1997a); "The nation's telephone companies have worked side by side with law enforcement for many years to provide them with surveillance technology and access to caller information. We take this responsibility very seriously and are committed to assisting law enforcement agencies with crime prevention and detection measures" (Roy Neel, president and Chief Executive Officer [CEO] of USTA, ctd in Miceli 1998).

[7] "I think the police [...] and other law enforcement bodies must always be able to catch bad men and bad women –such as they are– and they need the tools to be able to do that" (Regulation Officer and law enforcement liaison of large ISP industry association, Int10:5-7). See also Int11:9-11: "I think that communications interception has got quite a long history. It's been related to voice telephony until recently, so [...] the need is driven by the use people make of communications in society" (British Telecom Regulation Affairs Officer). For similar opinions see Int04:14-15, 17-18; Int06:11, 14-15; Int08:4-6; Int11:14-15; Int12:42-54.

> authorities might be [TUFF fraud and law enforcement liaison officer, UK, Int12:6-14; see also Int04:35-36];
>
> we have a role as corporate citizens to be co-operative and we're just as interested in helping law enforcement catch the crooks that use [...] our phone systems [CALEA Compliance Attorney, BellSouth USA, Int20:121-124];
>
> I don't think there is a company that we represent that does not agree that they have a social obligation to supply law enforcement with information on criminal activity [Technical Director of a US national telecommunications association representing more than 500 member companies, Int17:53-55].

Broadly speaking, however, the interviews showed that, both in the UK and the US, moral and civil duty considerations are more prominent in the public rhetoric, if not the decision-making process, of carriers than official documents tend to show[8]. Symbolic terminology, including phrases such as "common good" (Int04:303), "civil duty" (Int06:153), "good corporate citizen" (Int11:63; Int12:535), "social responsibility" (Int17:36) and even "national security" (Int16:117) were repeatedly mentioned during interviews as important ideological guidelines shaping the carriers' relationship with law enforcement:

> we get requests to run through our data to give them call data information [...], like, for example, when we had the [...] Olympic bombings here in Atlanta in 1996. We put forth a lot of effort. We ran call records from all the payphones around the Centennial Park, where the bombing occurred, to assist them in developing leads [.... W]e do a lot of things, [be]cause we are good corporate citizens. We try to [BellSouth USA CALEA Compliance Attorney, Int20:263-268].

Interviews showed that, in essence, UK and US carriers do not consider the practice of CI for law enforcement purposes to be fundamentally different from other public order provisions by centralised nation states, such as physical patrol policing (Int4:15-17), traffic policing (Int7:70-74), gun control (Int08:8-13), health and safety regulation (Int10:550-558) and emergency service provision (Int12:63-67)[9]. Nevertheless, UK

---

[8] In the UK, this has been recognised by the Information Commissioner, who has stated that, while communications data handovers remain voluntary, carriers are placed "under considerable moral pressure to co-operate with police" (ctd in Sutter 2001).

[9] "In other words, in a sort of parallel universe, policemen need police cars to go chasing bank robbers and chasing people exceeding the speed limit at the motorway; and nobody [...] has ever suggested to me that the police don't need police cars to drive around in. They should be allowed to do that. They should be allowed to break the speed limit if [...] it seems like a good idea at the time and jump red traffic lights and [all] that" (Regulation Officer and law enforcement liaison of a large UK ISP association, Int10:30-35). This analogy between CI and traffic regulation is often drawn in law enforcement literature on CI (see section 2.2.0).

carrier officials appeared more willing than their US counterparts to distinguish significant political implications in the potential abuse of CI, which inevitably sets the practice apart from public order provisions by the contemporary nation state:

> we're moving from an era where only the bad guys –in theory– or political subversives or whatever, but very few people [...] had anything intercepted [...], to one where everybody is intercepted on all their communications. Because they're going to do it; they're going to put this black box in here, it's going to be crammed in the switch and it'll be intercepting everything [CEO of large UK ISP, Int08:429-434; see also 191-196; Int10:42-48, 633-636; Int04:18-21][10].

This advanced awareness of the extraordinary social and political significance of CI use and abuse is often substantial and appears in the form of moral dismissal of overly aggressive CI practices and demands:

> I don't think we morally should [change our network technology to accommodate CI]. I mean, if you want my opinion, I think intrusive surveillance –in [...] the IOCA[11] terms– [...] a bad thing for society and that [...] BT –I can't speak for the Chairman of BT– [...] but I would find that morally difficult to cope with, if we were doing that [British Telecom Security Officer, Int07:212-215].

7.2.0. The Technological Promise of RIPA and CALEA.

Undoubtedly, the driving force behind the conception and implementation of RIPA and CALEA has been the realisation that the process of digitisation of telecommunications has largely taken place without consideration of law enforcement's CI requirements. Thus, it is the evolution of the technical features of telecommunications that has given rise to an extensive restructuring of CI in the digital environment, as represented by the aforementioned legislation.

Carriers on both sides of the Atlantic appear fully aware of the technological motivations behind RIPA and CALEA, whose "promise" (Int16:212-216) is to return large segments of the –now digitised– telecommunications realm to law enforcement supervision and control:

[10] Similar opinions appear to inform particularly the younger ISPs in the UK and one typically encounters it in industry responses to government consultation documents: "ISPs would like to be able to reassure their users that no automated set up of interception will be requested. Although more convenient to ISPs and absolving their employees from jeopardy on 'tipping off', automated interception would raise a significant 'Big Brother' image of the Internet" (Anon 1999a).

[11] IOCA was one of the previous "incarnations" (Akdeniz *et al.* 2001) of RIPA, as were parts of the Electronic Communications Act 2000 and the NCIS Code of Practice document (see ibid.).

> I don't think it's any secret that we already extensively assist the police services and [...] other people in this area. What this new legislation does, really, is [...] to put some new vocabulary and some new vernacular around something, which is happening already [British Telecom Security Officer, Int07:1-4][12].

7.2.1. The Ability to Intercept in the Digital Environment.

There is less certainty among carriers about whether the digital telecommunications environment is more susceptible to amplified and structurally seamless CI. Interviews appear to reflect the technical literature in this respect[13], by generating diverse views on the subject:

> nowadays, you will appreciate, [the network] is intrinsically ten times more, infinitely more transparent in some ways than it previously was [.... I]f you're talking about Internet technologies, then there's a huge amount of information stored, which the old analogue systems would not have [...] captured. [S]o it's [...] just intrinsically easier to see and, [in the] normal course of business, everything you can conceivably think of gets almost accidentally logged. I mean, computers nowadays [record] nearly everything. So [...] I can't see us having to change our network technologies to accommodate the RIP [British Telecom Security Officer, Int07:204-211][14];

> the trend is not towards networks that are easier to intercept; rather the reverse is true. The techniques needed for interception –finding where the packets are, specially identifying them, then duplicating them to special places– are not compatible with high-speed low-cost networks. Efficient and secure networks are inherently hard to intercept. Even if ISPs are currently able to intercept at the edges of their networks, those edges are blurring and moving ever outwards towards the customers themselves [Lansman 2000].

In the UK, many carriers –mostly ISPs– appear to be sharing the view of a number of civil libertarian activists who claim that "it is not possible to arrange anything like a comprehensive intercept capability" (Bowden 2000:667-670) in the digital telecommunications environment:

---

[12] See also Int20:281-289: "CALEA didn't change the substance of law. In other words, [...] what law enforcement has to do to convince a judge –what is [...] required for the judge to issue a court order– did not change [...]. All CALEA did was [...] it clarified [...] what carriers had to do to assist law enforcement in the conduct of electronic surveillance. And part of that clarification was that, as your technology changes in your network [...], technology has to continue to accommodate electronic surveillance. That's all CALEA did. It's a simple concept" (Bell South USA CALEA Compliance Attorney; see also Int10:252-263; Int012:268-269; Int16:212-216; Int18:33-39].

[13] See for example two competing opinions in Blacharski 1998 and Rozenblit 2000.

[14] For a similar view on the subject from a US standpoint see Anon 1997a. For a detailed analysis from an electronic security professional's standpoint, see Kampschoer 2000.

> [Planet Internet ha]ve had situations with police officers demanding actual web pages [accessed by] their customers [...], which would have been absolutely impossible for their size of customer base and also they wanted [...] complete details of emails or contents of emails going back to [...] 10 years or whatever –for as long as they've been operating. [That was] just technically infeasible. And, you know, the police officer thought "I can do this, because I have a warrant" [Fraud Control and Revenue Assurance Manager of large UK wireless communications company, Int04:181-189].

> With regard to carrying out interceptions in the 'middle' of larger networks, there is a unanimous view amongst industry experts [...] that such interception verges on the impossible and will certainly bear significant costs [Lansman 2000; see also Parish 1999].

In the US, where CALEA has been in the process of implementation for seven years, carrier representatives appear more prepared to overcome or bypass some of the more complex technological barriers to state-sponsored CI, providing financial resources from public funds became available:

> I think you need to tie up [technical and financial issues] together. Anything [...] is technically feasible. It's at what price is it technically feasible and who's going to pay for it? So, the simple answer is [that] anything could be done technically. It's how much do you want to pay for it and where do you get your money back? [Technical Director of a national US telecommunications association representing more than 500 member companies, Int17:160-161, 171-173];

> there are a few things that law enforcement wanted that [...] would affect carrier networks that [...] we pushed back for technical reasons. But you pour enough money on us and we can probably solve the technical problems [CALEA Compliance Attorney, BellSouth, USA, Int20:361-363].

Predictably, this view is supported by US law enforcement interests, who refuse to consider the technological complexity of digital systems as grounds for rejecting CALEA-compliant solutions (see Morris 1998):

> believe me, [CALEA] is not a technical nightmare for [carriers]. This is all well within their capabilities. That [...]'s never been a big problem. Other than the cost of doing, the technical ability to do it...all the packet protector whinnies are saying "hey, we can do this; we can do a lot more than that". Yeah, this is easy [FBI Special Agent, CALEA Implementation Unit, Int19:610-614][15].

Parliamentary records show that followers of this viewpoint are also to be found within

the British government. It would be safe to assert that former Minister of State, Charles Clarke, reflected a general policy principle of his Office when he stated in Parliament that he does "not accept the suggestion that the age of interception is over or that work in that area may be futile. That", the Minister of State continued,

> would be a philosophy of despair. I understand why people take that view –they see the Internet as an all-embracing vehicle that cannot be controlled by any national legislature. We believe strongly that the power of this form of communication and the nature of global crime in so many important areas, such as drugs, paedophiles and so on, is such that we must do what we can to control it. The powers in the Bill will allow us to have an impact on that. To say that we cannot do anything would be to accept a counsel of despair and we cannot accept that [HCSCF 2000].

Admittedly, this view interprets the advancement of state-sponsored digital CI as a matter of a series of primarily political, rather than strictly technical, executive policy decisions. The absence of specific technical information on the UK government's plans for digital CI under RIPA prevents a detailed evaluation of the technical feasibility of such plans. However, a leaked report produced by the ISPA through a secret ISPA/Association of Chief Police Officers (ACPO) forum in November, 1997 (Akdeniz *et al.* 1999)[16], showed that, according to network technicians, there were at that time very few digital barriers to digital CI that could not be overcome by technical means (ibid.). The report stated that, although technical improvements were required to increase the reliability of Internet-based CI, most of law enforcement's requirements[17] could be met, if the active co-operation of the relevant ISP, and the instalment of expensive specialist monitoring equipment, was financially compensated from public funds (ibid). According to Yaman Akdeniz, whose organisation, Cyber Rights & Cyber Liberties UK, publicised the leaked document, the report

> shows [...] that anything is possible –technically– to do. [ISPs] can monitor everything, [...] not only emails, but all sorts of wave activity, IAC [(Inter-Application Communication)]. I didn't know at that time that it was technically possible to [...] do all sorts of [...] activity [Int01:349-

[15] According to one UK industry representative, "in some instances we'd possibly be able to get [law enforcement] more [information] –what they haven't even thought of [Int04:178-179].

[16] The report, which was leaked to Cyber Rights & Cyber Liberties UK by an ISPA member, was produced following a series of secret briefings to ACPO about the ISP industry capabilities for the provision to law enforcement of information relating to the on-line activities of Internet users (see Akdeniz 2000).

[17] According to the report, such requirements include current or previous names and current content of email accounts, tracking Internet Message Access Protocol (IMAP) or Post Office Protocol Version 3 (POP3) messages through packet snooping, identifying IP addresses and monitoring customers' web site visitations, as well as newsgroup and Internet Relay Chat (IRC) activity (Akdeniz *et al.* 1999).

352].

Broadly speaking, however, it is likely that, while a number of barriers to interception might be overcome in the short term, the introduction of further, digitally enhanced service features in a increasingly competitive telecommunications market will certainly debilitate what now seem to be sophisticated CI models (see section 8.3.1):

> I think [the government ha]s set its agenda out and it's got a big wish list. And some of it will be possible, some of it will be possible but only for a very short period of time and other things will be "yeah, that's great to have" [Fraud Control and Revenue Assurance Manager of large UK wireless communications company, Int04:265-267].

Technical detail aside, it appears clear in interviews that carriers are aware that telecommunications digitisation has been anathema to state-sponsored CI[18]. This has not necessarily occurred due to intrinsic and inevitable security features in the digital environment, but rather due to the absence of law enforcement interests from technical debates on telecommunications digitisation. Industry interviewees on both sides of the Atlantic appeared well informed about the particular features of the digital telecommunications environment[19] that have denied law enforcement access to communications content and, often, even call data (Int04:267-272; Int08:410-413; Int10:22-24; Int11:284-286, 537-538; Int16:119-125; Int17:203-205; Int20:131-134)[20]. There also appears, among carriers, a certain apprehension of a number of emerging digital features, which are expected to pose drastic *cul de sacs* for CI, and whose emergence has been technically confirmed but has yet to be addressed by CI legislation:

> there is a need to change all this, but then the question arises: well it's all going to change again [...] within the next three or four years; how do you write legislation which has got to be future-proof, but is not just a blank cheque for the Secretary of State [...] to do what he feels like at the time? [British Telecom Regulation Affairs Officer, Int11:290-294];

> [t]here is no question that [...] the technological explosion that we're going through right now is going to continue even at a faster pace [...]. When we get fibre to the home, then what are you going to do? There's no [...] switch point; there's no place to put [a tap]. Are you going to

[18] For a legal-oriented analysis of law enforcement capabilities and technology-in-use see Standler 1997.

[19] Such features include voice-over-IP, multi-path, packetised voice communications, cellular and pay-as-you-go telephony, broadband and narrowcasting technologies, as well as call-conferencing, call-forwarding, speed dialling, voice dialling, automatic redial and radio pager technologies (see Appendix 3).

[20] In the UK, this comprehension of the digital barriers to state-sponsored CI is also evident in official responses from carriers to government consultation documents; see Anon 1999a and Anon 1999e.

> have [...] the government agency knock on your front door and say "I want to tap into your fibre system"? It just doesn't...it isn't going to happen. So [...] I think there are more questions that are going to be asked and there are very few solutions that are going to come forward [Technical Director of a US national telecommunications association representing more than 500 member companies, Int17:208-215];
>
> with ISDN coming up, with fibre to the home, I mean, it's kind of tucked into that. You can't go inside a person's home and run some beads out the back door [...] into a recording device [USTA lobbyist and CALEA point person, Int16:32-34][21].

Law enforcement interviewees acknowledged the relative incapacitation of traditional technical models of CI caused by the dynamics of digital telecommunications evolution. Interviewees in the UK confirmed rare public acknowledgements[22] by government and law enforcement representatives of serious setbacks to state-sponsored CI:

> I'm not going to say what our blind spots are, because I [...] wouldn't want the wrong people find[ing] out how to evade supervision. [B]ut I will say that in the [19]90s we suffered the most astonishing blows to our interception capabilities in living memory –certainly since I joined the Force [Former Special Branch Communications Intelligence Officer, Int02:110-114].
>
> BT has your number now, you decide you don't want BT any more, so you move it. And you go to Cable & Wireless and so on and so forth. Which means that [...], from a law enforcement point of view, it's a nightmare –you know? Who actually does own that number? And it's even worse when it comes to mobiles [Former Special Branch Officer, Int12:494-498].

In the US, law enforcement and intelligence services have been more willing to share such frustrations in public (see Morris 1998:n56; Freeh 1997b; United States Court of

[21] See also Int18:175-181: "I think the interesting thing about legislation and regulation is [...] that technology is constantly outpacing regulations and legislation and you can see with CALEA that [...] they never foresaw the [...] problems they're having with [information technology]. By the time the FCC gets a rul[ing] out on anything, technology has already far surpassed it and it's already dated. I have this feeling that by the time all of this gets sorted out in the courts they're going to have a whole new set of questions to answer [...] as we have all this convergence going on in the industry" (Government Relations Director of a large US national telecommunications association).

[22] Such instances include Todd 1999 and Veigas 1999. In 2000, the Interception Commissioner requested that a new warrant regime be considered for interception of messages for radio pagers (Command 4778), while a few months later the then Minister of State, Jack Straw, acknowledged that "part of the [RIP] Bill is designed to ensure that the intercept regime takes proper account of technological developments. One of those developments is that people change their telephones with a frequency that is sometimes astonishing, whereas, 15 years ago, it was a simple matter of one person, one line" (House of Commons 2000). Almost a year earlier, John Abbott, Director-General of the NCIS, recognised strong encryption as a "threat" to law enforcement's interception capability. "Now, we have an interception capability at the present time", said Abbot, "but we see it perhaps moving to redundancy unless we move legislatively and in practice we move forward to tackle the new technologies" (HCTISC 1999a).

Appeals 2000; Blair *et al.* 1995; Kallstrom 1997). In 1994, after receiving the analysed data of a nationwide survey on CI complications encountered by law enforcement in the course of investigations[23], the FBI leadership was concerned with "losing wiretap capability entirely" (Dempsey & Oram 1998)[24]. Even the NSA, arguably the technical and engineering vanguard of the US communications intelligence complex, has admitted that its operational capabilities are under threat by the digital telecommunications evolution:

> [w]e're behind the curve in keeping up with the global telecommunications revolution [...]. Our adversary communications are now based upon the developmental cycle of a global industry that is literally moving at the speed of light [...]: cell phones, encryption, fibre-optic communications, digital communications [NSA Director Lt. Gen Michael Hayden, ctd in Verton 2001].

US law enforcement interviewees described some of the more contested digital features of new telecommunications networks, such as voice-over IP, as a "huge can of worms" (Int19:526-527) and admitted to suffering from lack of technological foresight even following the implementation of CALEA:

> [when we were drafting CALEA], never did we think that telecommunications over a period of time –as we know it– would be supported by an ISP [FBI Special Agent, CALEA Implementation Section, Int19:531-532][25];

---

[23] Although the body of the survey was and remains classified, its summary results have been discussed in Congress and in a number of court hearings (see Boucher & Edwards 1994:§14-15; United States Court of Appeals 2000). Since then, the FBI has commissioned at least one more major follow-up survey on the social penetration of advanced digital telecommunications systems in the US (see Anon 1997b).

[24] Dempsey & Oram (1998) quote FBI Director Louis Freeh as stating: "we [the FBI] are missing a part of the playing field, but our position is that we don't want to miss the whole playing field". According to Diffie & Landau (1998:183, 274n), in 1992, the FBI's Advanced Telephony Unit reported that, in the absence of the implementation of a CALEA-type Act, the FBI would lose access to between 40 and 100 per cent of communications targeted for interception by 1995.

[25] This particular interviewee was in fact one of the first federal law enforcement agents to encounter CI barriers after the digitisation of large segments of the US telecommunications infrastructure in the late 1980s: "we became concerned about this when we observed these long periods of inactivity on the telephone when we knew [the targeted individual] was talking to someone on the telephone line. We could either observe it or we had [...] a microphone in there or an informant. We knew that he was using the telephone but for some reason our equipment was not working and not picking this up. I guess it first came to my notice when we've had prisoners [...] in a local penitentiary there making calls to an associate only to be conferenced by that associate to a third party. And the associate would then drop out of the conversation or [...] would hang up his phone [.... O]f course, the wiretap would be on the associate outside of the prison. And we would be left high and dry with no content of the conversation, while all of the time knowing that he's talking to a drug associate or something and that the conversation was being supported by these associate's facilities and services at the phone company. We would [...] certainly get the billing record of it, but we had no idea what was said" (Int19:30-38).

> [a]fter CALEA came about, there was a huge sigh of relief [...]. We thought we had it covered. And then, about a year later, our consultants started calling us with [...] news that some ISPs were moving into the voice telephony market [First Class Sergeant, Communications Officer, United States Special Forces, Int14:89-92].

7.2.2. Law enforcement's Knowledge Gap.

Particularly prominent in interviews with UK industry representatives were manifest negative attitudes over what many perceive to be an absence from law enforcement operative standards of even basic technical knowledge about telecommunications:

> law enforcement people [usually] turn up with a bit of paper asking for something in gobbledegook, because they don't understand, or turn up and, as a lot of people in the industry say, their first words are "I don't know anything about the Internet, but can you do this or that or the other for me?" [...]. I was talking to somebody yesterday, who [ha]d been taken along to one of [law enforcement's] operation centres that deals with this kind of thing and they were just amazed [by] how out of date everything was, how it was all –you know– how unsophisticated it was. And [...] this is what you're likely to find, rather than all of us being spied on by secret satellites that can read our number plates from five miles in the air. I think that most of the time you'll find that police [officers] don't even understand that a '.com' email address [...] is something to do with the United States [Regulation Officer and law enforcement liaison of large ISP association, Int10:328-332, 347-355; see also 344-347; Int4:191-193].

According to interviewees, the underlying reasons for this phenomenon are primarily cultural, and have much to do with the casual pace of change that is characteristic of bureaucratic governmental institutions in large-scale social systems. In other words, law enforcement bodies have been given little incentive by government to change their investigative and organisational routines:

> the police are [...] almost virtually seen as not moving on in their thinking about crime from the [19]60s or [...19]70s. Sometimes you feel as if [...] they're only really interested in that type of [low-tech] crime. When it comes to more technical crime, because it's more to solve or more difficult, they can't possibly [...] solve it themselves [Fraud Control and Revenue Assurance Manager of large UK wireless communications company, Int04:58-64];
>
> the police [...] still –by the way– refer to us [as the] GPO [(General Post Office).... T]he[y] still phone us up and say "is that the GPO?". And that is [laughs] and that was before I joined the company –it was the GPO. [M]ost policemen think that the Post Office deals with the post and that the GPO deals with the phone. And so, they are so far removed and they don't understand what's happened[; a]t the working level in the police

> forces they have no clue as to what's happened. They just assume that everything is as it used to be [British Telecom Security Officer, Int07:237-246].

This belief is generally shared by UK civil liberties lobbyists[26] and appears to confirm similar opinions that permeate written responses by carriers to the UK government's IOCA consultation document (Sutter 2001)[27]. Recent articles in the specialised and popular press explain that the "lack of technical training and expertise among law enforcement officers" is a "major concern" (Delio 2001) for the UK ISP industry:

> [a]t the moment, the big problem Internet service providers have with the police is their stupid questions. After a while, it gets expensive and unproductive. It's a problem. It's always a problem, and it's a very serious problem [Tim Snape, ISPA member, ctd in Delio 2001; see also Anon 1999a; Anon 1999b].

Accordingly, numerous UK ISPs have requested that, prior to fully implementing RIPA, the British government proceed to train[28] law enforcement officers sufficiently on CI-relevant technical issues:

> ISPs would expect to deal with technically competent [law enforcement] staff, who are aware of the relevant Internet protocols and their properties. We are not in business to provide free training for law enforcement. Our experience in the past is that this is an important practical issue and the government should consider making the use of centralised expert assistance, from NCIS or elsewhere, mandatory when a local police force wishes to implement an interception order [Hall *et al.* 1999; see also Anon 1999b; Perry 1999; Weatherall 1999; Wraith 2000].

---

[26] "They [...] don't really understand or they seem to have difficulty understanding –putting themselves in the shoes of the Internet user [...]. When one hears [...] very senior policemen talk about their approach to the job and how they're going to want to police cyberspace, you [...] think they're really living in another [time –]50 years ago. Or, at least, [that] they're not projecting their minds forward to ten years from now" (Bowden 2000:380-381, 426-429).

[27] Even though such attitudes did not surface in interviews with US industry officials and do not appear in the US literature on the subject, it should not necessarily be assumed that US law enforcement agencies enjoy a higher degree of approval from carriers when it comes to their technical expertise. During an investigation case that I witnessed in the US, in July 2001, law enforcement personnel demonstrated shocking lack of CI-related knowledge. It took law enforcement officers and criminal investigators working on the case more than two weeks to trace the originator of a malicious telephone call. Furthermore, the officers in charge of the investigation were completely clueless as to the process of initiating a telephone call trace or installing a wiretap.

[28] UK law enforcement officials have, in certain instances, acknowledged this lack of technical expertise within their ranks. In 1999, John Abbot, Director-General of NCIS, stated that, "we do have strategic intelligence analysts and [...] some experts, but I would not wish to suggest that we are over-endowed with people who understand the details of this [...]. We do have 'techies', both in-house and out-house, that we can use to assist us. It would be remiss of me to suggest that we have them in sufficient numbers, of course, but we are flexible. We recognise that there is a need to move forward" (HCTISC 1999a). At the moment, the only such law enforcement training facility in the country

7.3.0. Shifting the CI Paradigm.

Some UK ISPs have insisted that it is indeed the lack of technical understanding by law enforcement of digital telecommunications networks, as well as their refusal to engage in sophisticated technical training, that ultimately shaped the British government's RIPA methodology (Anon 1999a). Hence, instead of opting for a CI model based on network backbone interception by law enforcement agencies, the UK's RIPA strategy appears to be to "spread the pain out and [...] require every ISP to maintain some sort of interception capability" [Bowden 2000:650-655].

This interception model, which, as explained earlier (section 6.3.1), characterises the basis of both RIPA and CALEA, implies that, for the first time in the history of CI, 100 per cent of a wiretapping operation has to be performed by the carrier (Yarbrough 1999:§6; Kerr 2000; Charney & Alexander 1996). Both law enforcement and carrier interviewees appear to recognise this crucial paradigm shift in CI:

> [i]t used to be [that] we'd provide the logistics –the information on the subscriber's line– and [...] that was it –we'd never hear from them again, unless something went wrong or whatever [...]. Now [the carriers] will have to do everything –they'll have to tap the line on the screen and either route [the intercepted data] to a separate location or even record it themselves. And [then] they'll have to untap [the line] when they're told to do so and –you know– everything shifts to the carrier [Former British Telecom external maintenance engineer, Engineering Division, Int02:481-488; see also Int04:244-247; Int07259-261; Int12:559-560; Int16:186-193; Int21:122-123];

> for the [...] drug dealer, the paedophile and that type of person, even down to the racist, to the football hooligan –that sort of activity– yes, they do need telecom industry input, because they haven't got the resources otherwise. They won't [...] use the large resources on those type[s] of people. And, you know, without telecom[munication]s' input [we] would just turn out the light [Former Special Branch Officer, Int12:565-569];

> you know, for years, we would be out climbing the telephone poles. We would be out in the cross-connect boxes [...] and we would be armed with information they provided us over a phone call, saying, "hey, Joseph's phone lines are here at this intersection. [They are] at this particular box on the ground there and if you go to cable number" so on and on, this number...this number "and you clip onto them you'll hear Joseph talking". I'd go up there [...] or send my guys out there, we'd clip on a clipper and then the carrier is none the wiser. I mean they know that it

---

appears to be operated by the Special Operations Unit of the West Midlands Police Constabulary (see Watson 2000; Wraith 2000).

> probably is out there somewhere but they're not doing it. And it was pretty much...you'd wash your hands clean of it. Now –wow– it's completely different in several respects: one, they have to do all the work. I call them up [and] say, "look, I need this intercept. You've got 'x' number of days to get this thing up". And they're struggling to do the work in their switch –with some keystrokes. And they're held directly liable to the courts. We're not doing anything. Say they're not doing it correctly and hook it on to the wrong person. It's their problem, yeah. So the shift of labour is [...] going to be dramatic [FBI Special Agent, CALEA Implementation Section, Int19:652-669].

7.3.1. CSPs as Guarantors of CI Legality.

In the US, the FBI has gone to great pains to draw a firm line of distinction between the act of technically implementing a CI request and the act of qualitatively evaluating its necessity. According to the FBI, the fact that the carriers' role will be more ingrained in the mechanics of the CI process does not entail that carriers can assume the responsibility of assessing the justifiability of CI requests:

> [it should not be] suggest[ed] to carrier personnel that they are supposed to test the legal process [of CI operations] against some 'look up table' of statutes, which are often somewhat complex, and then substitute their review for that of a judge when a carrier is presented with a facially valid court order. Carriers are the implementers, not the enforcers, of lawful intercept orders, authorisations, and certifications under the electronic surveillance laws in this regard [Morris 1998].

There are numerous signs, however, that carriers are already being drawn into a more active and engaging legalistic role in CI operations, which is a direct outcome of their upgraded functional role in the implementation of CI orders. In the UK, BT has already requested assurances for the personal safety of any of its employees "involved in security-sensitive cases, such as those involving terrorists" under the RIPA (Stewart 1999). Additionally, interviewees both in the UK and the US suggested that carriers are already drawn into court battles as witnesses against CI targets prosecuted by the authorities:

> I have even reached the point of giving [the police] my personal information –my date of birth, name, etc– because the [intercepted] data I gave them are going to be used as an exhibit in a court case and I need to be there and confirm it [Fraud Liaison Officer of the UK branch of large telephone and Internet service provider, Int09:235-238];

> yes [we co-operate with law enforcement], quite regularly –most notably [with] the Computer Crime Unit. We've had quite a lot of involvement

> [in] helping them with gathering evidence –that kind of thing [Fraud Control and Revenue Assurance Manager of large UK wireless communications company, Int04:129-130];
>
> if we're out there installing the taps then [we are] sometimes required to testify in court that we did do so and that, as far as we're concerned, we got the right individual [or] group of individuals [...], that we heard them speak the words recorded and so on [...]. Now [the carriers] are gathering the data on our behalf, so, yes, their people will be called [...] to appear in court and confirm their role in the operation [First Class Sergeant, Communications Officer, United States Special Forces, Int15:37-43].

It is not surprising perhaps that, faced with such a high degree of engagement in CI operations under RIPA and CALEA, UK and US carriers are beginning to query the justification of CI requests:

> I want to hear some background. I want to know the seriousness of the crime so I [can] decide how much of my resources I'm going to make available. This is manpower, right? If you tell me [...] "this guy is up for murder, we believe he [...] did the whole thing off the Internet", [then] all right, we'll just sit here and see if we can do it now. Right. That's different [...]. But, occasionally, guys come here with a warrant [...] and it should be: "have you got a warrant?" and [if] you've filled it out wrong [then] this is a violation of my client's human rights. Or you may [...] have filled the form in right but you don't have enough justification [...]. Yeah, you filled in the form, you've got all the boxes right, but you've asked for this [much] whereas the crime is only that [small]. [So], my client is not going anywhere. He has got rights [and] you haven't shown me enough justification [CEO of large Internet service provider, Int08:309-311, 340-349][29];
>
> by virtue of the services and features we provide, in the future, electronic surveillance is going to have to be conducted out of the switches as opposed to on the [...] lines out of the switch. [It]'s going to be controlled by us, so I think that does compress the potential areas of compromise. And so I think that makes it more secure and more private [CALEA Compliance Attorney, Bell South, Int20:293-296][30].

In a 2000 presentation before a large group of law enforcement liaison officers of UK wireless and wireline carriers, the UK telecommunication industry's designated Single

[29] See also Int11:381-384 and Int12:276-282: "in the past, there has always been a break –i.e. the industry has done one thing, be it that it has to have a warrant– but really at the end of the day we've no idea why that warrant was served or why that warrant was invoked. Where[as] here we are starting to get a much clearer picture as to why we're being asked. And if we're not happy, the procedures are there for us to go back and say "I'm sorry, I don't know what your warrant says, but [...] unless you can convince me that I'm not breaking this rule, this rule, this rule, then I 'ain't' executing" (TUFF fraud and law enforcement liaison officer, UK).

[30] See also McHugh & Cordwell 2000: "[under CALEA, carriers] will be responsible for ensuring that 'appropriate legal authorisation in the form of a court order signed by a judge or magistrate authorising or approving interception of wire or electronic communications pursuant to 18 U.S.C. Section 2518(7), or any other relevant federal or state stature' has been received".

Point of Contact under RIPA, Jack Wraith, characteristically described the new, upgraded CI role of carriers as guarantors of CI legality:

> [t]he nature of [a RIPA CI] enquiry is in detail. What material benefits [are] the law enforcement seeking to gain from this request? [W]hat these new procedures are doing, is starting to make them sit back and identify why they are asking. If it happens that the procedure has not been followed and if you have suspicions along those lines, then it is up to you to bring them to our attention, and the necessary investigations can take place and, if necessary, the wrongs will be made right [Wraith 2000].

To a large extent, this novel attitude stems from the carriers' need to safeguard their legal status by ensuring that, while fulfilling law enforcement requirements under RIPA and CALEA, they are also able to meet the privacy demands of their users[31]. Failure to do so could potentially compromise revenue. Carriers on both sides of the Atlantic generally appear to view the increased burdens placed on them by new CI legislation as efforts by government and law enforcement to make them not only technically, but also legally responsible for CI in the digital telecommunications environment, in terms of privacy laws:

> it's a pendulum and we're sitting in the middle. If it all goes wrong [...] – say there [are] two big buckets of water and you say "I was wrong"– we know who's going to get wet [CEO of large Internet service provider, Int08:337-339];

> [a]fter three years of futile negotiations, the industry is caught in the middle and faces massive sanctions despite our good faith efforts to implement the [CALEA] statute [President and CEO of USTA ctd in Miceli 1998].

7.3.2. CSPs as New Trenches of Communications Security and Control.

This new positioning of carriers at the operational centre of models of CI practice in the digital telecommunications environment is arguably more significant than it may initially appear: it should be expected that, under this new regime, carriers will be seen as crucial brokers of influence and control by groups or institutions wishing to either increase their CI capabilities or augment the security of their communications. The UK-based Alliance for Electronic Business (AEB) has correctly remarked that, under a CI model whereby

[31] This applies particularly to the UK, where civil liberties organisations (Int01:239-244), carriers (Int08:225-230) and even law enforcement themselves (Gaspar 2000:§7.1.1) have acknowledged that certain elements of the RIPA clash with the Data Protection Act 1998 and the European Convention on Human Rights (ECHR) protocols.

all carriers and service providers are required to facilitate state-sponsored CI, the risk of abuse could be substantial:

> [a]ny system capable of intercepting and understanding communications could become a target for those working outside the law [Anon 1999e][32].

Reflecting AEB's concerns, some UK carrier interviewees pointed to the considerable potential of telecommunications employees being in a position to systematically undermine CI investigations and even questioned the trustworthiness of their own staff:

> **Q:** Do you think that there are individuals operating within telecommunications companies on behalf of criminal syndicates?
>
> **A:** Of course, of course, primarily [...]. Especially engineers.
>
> **Q:** Are you sure about this?
>
> **A:** Yes, indeed. In the past there have been cases of carriers where insiders were assisting criminal elements [...]. Do you realise how easy it is to be working for a [carrier] company and [...] lending a hand to criminals in return for a commission? I caught a guy here once; I certainly did [Fraud Liaison Officer of the UK branch of a large telephone and Internet service provider, Int09:156-165, 366-368];
>
> it's not beyond the boundaries of imagination that you've got a Mr Big. Our local Mr. Big is a couple of blocks away. He drives around in a great big car, has loads of money, but the only income he's supposed to get is £400 a month. Now, if our local Mr. Big was kind of concerned about what he was doing and was using us as an ISP, it wouldn't take him long to work out who the man that handles all the logs and things is, who's the only person that's authorised to turn the key on the black [interception] box and download the data. So it's not [...] going to be hard for him to make sure that that guy [...] gouges all the tapes and he puts them in the cupboard; or gets the tape and replaces it with a little blank one and changes the label; or forgets to do the backup on his messages –you know? [CEO of large Internet service provider, Int08:386-395; see also Lansman 2000].

Although some US carrier officials, too, have alerted to the potential of internal, carrier-based undermining of state-sponsored CI operations[33], US telecommunications and law enforcement officials appear to be more worried about the prospects of large criminal cartels or adversary intelligence organisations actually purchasing locally-based CSPs in

[32] AEB's concerns are not unsubstantiated; the Head of BT's Security Department has admitted that his Department spends "a third of [its] time and resources on looking at [BT's own] employees who are allegedly dishonest" (Bleep 1992).

[33] "In a packet [communications] world, somebody has to open the packet to look for the information the FBI is seeking. Is the FBI going to do it [...]? Who is going to be looking over everyone's shoulders when we open up this information?" (Grant Seiffert, Vice President of External Affairs and Global Policy, US Telecommunications Industry Association [USTIA], ctd in Brown 2001).

order to shelter their communications from state-sponsored CI:

> in effect –I've made this comment to the Bureau that I'm sure they were well aware of– since the Telecom[munications] Act of 1996 has come about, who is to say that drug dealers or the mob cannot go out and create their own –or have not gone out and created their own– competitive local exchange carrier? They can do that themselves. I am sure they have thought of that. It would take a lot of financial resources to do that, but you're talking about folks that have strong financial backing. They launder a lot of stuff [CALEA Project Manager of a large US telecommunications carrier, Int21:146-151][34].

Indeed, an FBI Special Agent interviewed for this project revealed that there has already been at least one case where a local exchange carrier has been targeted and purchased by organised criminal interests wishing to communicate in a CI-free environment:

> [w]e've actually seen the Mafia –the Italian Mafia– purchase a telephone company in New Jersey –the whole telephone company. Now, how are we going to tell that? You can't just knock on the door and say "we've got this court order and we were wondering if you could help us, but don't tell anybody" [FBI Special Agent, CALEA Implementation Section, Int19:716-719].

Notably, the FBI has remarked in Congressional hearings that it expects foreign ownership of US-based telecommunications carriers to have a negative effect on CI operations, because foreign-owned carriers would not necessarily be expected to share the US law enforcement and intelligence community's sense of safeguarding 'national security' and 'public safety'[35].

Ultimately, it should not be presumed that concerned UK and US state institutions, including law enforcement, are content to place increasing CI operational burdens on privately owned telecommunications carriers. This paradigm shift, which can conservatively be characterised as dramatic, signifies a relative loss of control by state institutions of the micro-mechanics of the majority of domestic CI. FBI sources have already expressed regret over this and have admitted that

---

[34] In the UK, service provider ICL has raised this very issue with the government: "[w]e can expect smaller and smaller organisations, even individuals, to operate their own e-mail systems rather than relying on ISPs. It is likely that conspirators will operate their own services too, thereby either hiding key messages from surveillance or warning the targets of the surveillance. Any interception is going to have to rely fundamentally on the trustworthiness of the ISP and we expect this assumption to become more doubtful over time" (Emery 1999).

[35] "A [...] significant area of concern [for the FBI] is the security of US intercept and data acquisition activity [...]. Without adequate safeguards, the damage to an [interception] investigation would be done almost from the moment the US serves process on the foreign affiliated carrier" (FBI General Counsel Larry Parkinson's testimony in STTCPUSHRCC 2000; see also Anon 1997b).

> [b]ecause law enforcement no longer has direct access to the intercept point, it can no longer determine for itself on a continuous basis whether the delivery channel or circuit is operating properly [Yarbrough 1999; see also Morris 1998; Blair *et al.* 1995].

In interviews with law enforcement officials, in both the US and the UK, it clearly emerged that they are in considerable discomfort over the loss of the detailed management of CI operations:

> changes in technology [...] mean that we have, in essence, lost control over a tool [that is] crucial to us; we can still get it done –hopefully– but we're not the ones doing it [...]; we are effectively sub-contracting [...]. Is this [a] change for the better? I'd be hard-pressed to say "yes" [First Class Sergeant, Communications Officer, United States Special Forces, Int15:67-71; see also Int19:681, 703];

> I mean, you don't really know these [carrier] companies –you have no idea who they are, who they work for. Security will be compromised –no question about it [.... It is] only a matter of time [Former Special Branch Communications Intelligence Officer, Int02:404-406].

7.4.0. The CSP / Law Enforcement Interface Under RIPA and CALEA.

The close historical ties between law enforcement agencies and telecommunications carriers or service providers in the US and the UK were discussed in detail in chapter five. This was indeed confirmed in numerous instances by law enforcement and CSP interviewees on both sides of the Atlantic (Int02:93-96; Int09.263-265; Int10.332-333; Int17.142-144; Int18.61-62; Int19.447-449; Int21.22-25; see also Anon 1999c).

Both in the UK and, especially, the US carriers have traditionally endeavoured to retain an "arm's length" (Int21:39) distance from law enforcement institutions, and it is too early to determine whether this distance will be retained in the post-RIPA and -CALEA environments. Both carriers and law enforcement representatives appear to recognise that their institutions are, in a sense, "compelled by legislation to work together" (Int06:163-166):

> [t]he combined efforts and collaboration of the industry and the law enforcement agencies will likely be required on a continual basis for the foreseeable future as the nation's communication infrastructure undergoes a nearly complete metamorphosis (Blair et al. 1995; see also Veigas 2000).

In the pre-RIPA and -CALEA environment, the relationship between law enforcement and carriers was not a particularly defined process (Int07:186-187), and it has generally

been maintained through a variety of informal connections, including personnel exchange between law enforcement criminal intelligence and telecommunications security departments (Int09:343-345; Int14:213-216)[36] and even through broader projects, such as British law enforcement's Joint Co-operative Community Approach (Int07:190-193). There are signs, however, that under RIPA and CALEA the relationship between the telecommunications industry and law enforcement will assume an increasingly more structured and defined format.

This process has been initiated through the negotiations between law enforcement and industry that preceded or followed the implementation of digital CI legislation. In the US, most such negotiations[37] were facilitated by the Electronic Communications Service Provider Committee (ECSPC), an industry/law enforcement forum specifically created in 1992 to address digital barriers to traditional models of state-sponsored CI. The forum, which held its first meeting at the FBI's Quantico, VA, facilities sometime between March and May 1992[38], operated under the auspices of the Alliance for Telecommunications Industry Solutions (ATIS), and became part of Telecommunications Industry Association Standards Forum (TIASF), following the implementation of CALEA (Morris 1998n15). The FBI has acknowledged that the ECSPC served as the platform for "literally hundreds of meetings" between law enforcement and industry representatives (Kallstrom 1997; see also Freeh 1997b).

In the UK, three groups are still active as vehicles of contact between law enforcement and industry actors engaged in negotiations over the RIPA. By far the most influential of those is the Joint ACPO, ISP and Government Forum[39], which preceded by more than

[36] "If you want an investigator it will cost you the Earth to take a man [sic] off the street and train him [sic]. If you want an investigator into telecom[munication]s, there is no such animal. So what you do is you say "well, what's easiest?". The easiest is to bring them on board and bring them up to speed in terms of the telecom[munication]s side, so let's take an investigator who has cut his [sic] teeth in law enforcement, be it customs, be it police, be it intelligence, and has those skills –those investigatory skills. And add on to those skills what is necessary [...] for him [sic] to understand telecommunications and you've then got a telecom[munication]s investigator. So, by virtue of that, you will find a great deal of law enforcement coming into the industry as opposed to the other way around. In other words, the flow tends to be one way" (Former Special Branch Officer, Int12:543-552).

[37] These negotiations were unsuccessful and convinced the US law enforcement and intelligence community that the telecommunications industry was not willing to voluntarily facilitate CI. This realisation led to the emergence of CALEA.

[38] The existence of the ECSPC forum was only revealed after government documents were released under the FOIA, but details of its activities have remained classified throughout its existence. The FBI has released the forum's initiation date as 14 May 1992, whereas independent observers claim that the group met a few times before that official date (Morris 1998n15; Meeks 1994).

[39] See section 7.2.1n14.

two years RIPA's enactment by the British government. Ever since its formation, the forum has held regular meetings with the objective to

> develop and maintain a working relationship between the ISP industry and law enforcement agencies in the UK, such that criminal investigations are carried out lawfully, quickly and efficiently while protecting the confidentiality of legitimate communications and with minimum impact on the business of the Industry [Pearson 1998; see also HCTISC 1999].

The ACPO Police and Telecommunications Industry Strategy Group is another forum that has served as a platform for negotiation between law enforcement and wireless industry representatives concerning the RIPA[40]. In a recent leaked NCIS report, NCIS Director, Roger Gaspar, asserted that, through the ACPO and Telecommunications Industry Strategy Group, industry and law enforcement actors have "developed a strong strategic partnership" (Gaspar 2000:§4.1.3)[41]. Parallel meetings between the law enforcement and intelligence community, on the one side, and ISPs on the other, are facilitated through the Internet Crime Forum (ICF), a group which aims to "develop and maintain a working relationship" between the two sides (Perry 2000b; see also Perry 2000a; Int10:391-395).

Regardless of their legislative and practical accomplishments, the above groups have served as vital channels of recognition and mutual identification of individuals on both sides, who have been instrumental in creating and implementing the operational and legislative CI models incorporated in RIPA and CALEA. According to one ICF member, the fundamental meaning behind these negotiations is that

> if people need to get hold of one another, there is quite a lot of recognition –if you like– between people like myself and law enforcement people. So, if you needed to go and get an opinion about something to do with law enforcement [...] you can just [...] pick up the phone and talk to them [Regulation Officer and law enforcement liaison of large ISP association, Int10:397-398, 401-405; see also Watson 2000];

> I guess the good thing that came out of the ECSP[C] meetings was a networking of contacts within law enforcement [and] within the telecom

[40] The Group brings together representatives of "BT Cellnet, One-to-One, Orange and Vodaphone. It also has three PTOs [(public telecommunications operators)]represented in the form of BT, Cable & Wireless and MCI WorldCom. There is [also] a representative there from the FCS [(Federal Communications Services)]" (Wraith 2000).

[41] According to its official statement of purpose, the Group aims "to examine the strategic relationship between the police service and the law enforcement agencies and the telecommunications industry, in particular with respect to criminal-related matters" (ctd in Wraith 2000).

> industry, that followed through for the next few years as people would call [and] contact [each other] once CALEA was passed [FBI Special Agent, CALEA Implementation Section, Int19:72-75; see also HCTISC 1999].

The enactment and gradual implementation of RIPA and CALEA is also expected to increase common educational seminars and training schemes between law enforcement and CSPs:

> we'd certainly be looking to do more [common training]. And there [are] lots of avenues to achieve that by TUFF. There's also an annual conference [that] FCS and TUFF run for law enforcement and European law enforcement, so there [are] lots of opportunities there [...] to network, plus to [...] do the training side [Fraud Control and Revenue Assurance Manager of large UK wireless communications company, Int04:198-202; see also Int04:166-170; Int10:526-527, 383-387; Gaspar 2000:§4.1.2];

> [y]es, [...] we'll be seeing much more of them and they'll be seeing much more of us. It's been like this for a few years, but now it's going to be more specific [...]. It's going to be less [of] "are we going to implement CALEA?" and more of "[...] what's the most feasible way [to] do intercepts under CALEA?" [First Class Sergeant, Communications Officer, United States Special Forces, Int14:222-227].

7.4.1. Exchanging State Monopoly for Chaos.

Admittedly, one of the most fortified digital barriers against CI has not been technical, but rather regulatory. It has long been recognised that the expiration of large, state-owned and -protected telecommunications monopolies, which occurred in the 1980s[42], has been directly responsible for an equally dramatic break up of the compact community of law enforcement and telecommunications security officials. In the UK, the astronomical increase in the number of telecommunications carriers and service providers –more than 200 PTOs and several hundred ISPs, according to recent estimates (HCTISC 1999a; Wraith 2000)– has virtually brought certain areas of state-sponsored wiretapping to a halt (Int02:121-124)[43] and carriers are certainly aware of this:

---

[42] In the UK, the process was initiated in 1981 and had been completed by the summer of 1993, when the UK government reduced its BT holdings to nearly zero, so that BT became fully privatised (Spiller & Vogelsang 1996:95). In the summer of 1993 the government further reduced its holdings almost to zero so that British Telecom is now fully privatised. In the US, the process began in 1980 and had been completed by 1991 (Stone 1989:11; Cohen 1992:3ff).

[43] Indeed, UK ISPs have been known to aggressively use the absence of any meaningful regulation of the ISP industry as a weapon against the government during negotiations over RIPA: "we don't need a

> [w]ithout doubt, it is a huge problem. Quite often [we] may be the second or third call that a policeman [sic] has made trying to identify who owns a particular CLI [(Calling Line Identifier)] or complete service operator. So, sometimes I wouldn't envy their position –they just can't locate who the service provider is now [...]. It's [...] a problem [and] I am sure it is going to get worse in the future [Fraud Control and Revenue Assurance Manager of large UK wireless communications company, Int04:208-211, 220; see also Int07:227; Int10:468; Int12:369-370][44].

In the US, law enforcement officials have not hesitated to describe the deregulation of the country's telecommunications sector as "dramatic" (Yarbrough 1999), "vastly complicating" (Boucher & Edwards 1994) and "chaotic" (Blair et al. 1995) from a security viewpoint, while industry representatives have asserted that the sheer number of new CSPs in the deregulated market means that agents in the US government "are looking at a nightmare in administrating CALEA" (Donald Bender, USTA CALEA Officer in Auble & Bender 2000). Indeed, law enforcement interviewees in the US overwhelmingly confirmed the seriousness of these fears:

> [t]he dynamics [...] of the thing are so varied –and if they are not directly related to CALEA itself, they're related to the number of players that are now in the telecom[munications] world [.... T]he paradigm broke [with] the [...] Telecom[munications] Bill of 1996, which allowed every entrepreneur to enter the telecom[munications] market. I just cannot convey to you the volume of people, who know nothing about telecom[munication]s, that have jumped into the market. And, as a result, everything has been bought up, absorbed or split up and there are so many players. The vast majority of the people now are not sure what their responsibilities are. [And] it's not just a dozen carriers we [...a]re working with; there are 37,000 carriers. Half of the carriers today did not exist in 1994. It's that big [...] change [FBI Special Agent, CALEA Implementation Section, Int19:757-761; 806-809; 817-819; see also Int20:155-158, 205-207; Int21:144-146];

> [b]efore the break up [...], say, five years ago, it was all local people that I dealt with and it was all people that [we] knew [...]. And they [...] could help me at two o'clock in the morning as well as they could at ten o'clock in the morning. Because they knew who I was, they didn't have to get clearance. After [the carrier] relocated –see, they got bought out– [...] to North Carolina, a lot of times when we have problems and call in they don't even know [who and] where you are. They want to know where you

---

license to operate our network, so blackmail in this case will simply get you unwanted publicity" (Parr 1999; see also Int05:533-539; Int08:62-64ff).

[44] "[Law enforcement] would probably start with [...] the BT books that say CLI ex –this geographic region– and this is a number owned by[, say,] Cable & Wireless. So they phone Cable & Wireless [and] Cable & Wireless say "no, this has been passed on or ported on to", say, "Energis". They phone [Energis] and then [they] say "well, actually, we've actually put this on through an [...] account and you need to phone this number". So [...], at minimum you're talking about three or four calls. So it can be a bit of a problem" (Int04:213-218).

are [Technical Unit Chief, Emergency Communications Unit[45], Int13:145-151][46].

7.4.2. CI in a Global Deregulatory Environment.

Law enforcement and industry officials have also alerted legislators to the fact that global deregulation developments in the field of telecommunications could mean that CI interception facilities could be based in the territory of a country other than the country where state-authorised CI is sought. Hence, nationally valid-warrants could be increasingly rendered invalid in a rapidly global telecommunications environment:

> [i]t is vital [...] that a [carrier] company [...] maintain within the United States interception access to the stored wire and electronic communications of their US customers and subscribers and any records and subscriber information relating to such US customers or subscribers. If such information is unavailable because it is stored beyond the US' borders, subject to restrictive disclosure laws of foreign countries, or technologically inaccessible, the national security, law enforcement, and public safety interests of the US are degraded proportionally [STTCPUSHRCC 2000; see also Blair *et al.* 1995];

> [y]ou know what [could happen]? [Carriers] can put the [switches] in another nation. And that's a real...now you're jumping not only to technical problems, but [also] to legal problems. Think of this: "why don't we put [them] in Tijuana, Mexico? Labour's cheaper, it's pretty close to our copper". Now, could I have gone down to Tijuana with a US-issued court order [...] for a drug case? Oh, man, they're going to laugh me right across the border. So, that's creating a lot of heartache for law enforcement [FBI Special Agent, CALEA Implementation Section, Int19:641-647];

[45] Name of institution withheld by interviewee's request.

[46] "You've got [...] fourth parties now. Here we've got one supplier that is buying his lines from a guy that bought them from Sprint [...] So when we have a problem with a call and we go back to Sprint, Sprint says 'well this is Rogers Communications'. So we thank them and we call Rogers Communications and they say 'oh yeah, we'll help you out. Oh, I'm sorry, we sold that to Larry Communications. We don't have any record of that'. Who is Larry Communications? 'Oh, well...well, I'm sorry, I can't tell you that; that's confidential information. You have to get a court order and I'll give it to you'. And, I mean, this could take forever. You've got to get a court order. You've got to find a judge, you've got to prove to a judge that you need [...] this information and he's not going to give it to you because of who you are and who you work for. He's not going to do anything, because he doesn't want to get in the middle of a lawsuit. So I've got to prove to him that I've got to have it. And [...] this has got to happen quick, because there might be a man that has called in because somebody is in the other room killing his family and we can't figure out where he is at. We can hear all this commotion going on and we start tracing and we just run into dead ends. We didn't use to have that. There were no third parties [...]. Once it almost cost us dearly; and I say 'almost' because at the last second somebody [from the carrier] went around all the red tape and said 'listen, I believe that if you go out to Joe Smith's you'll find that that's where this phone goes'. A few times we've done that. It was a real emergency and nobody went back through the channels to figure out how we knew what we knew. They figured it's just police emergency, everybody thinks they know that we know where everybody's at. So nobody checked. But we don't know where they're at" (Int13:108-123).

> Demon Internet already operates a network with equipment in three countries and has plans to operate in further parts of the European Union. Some parts of the user access infrastructure for the Netherlands are in fact physically placed in the UK and at times UK infrastructure has been housed in the Netherlands [...]. Is a UK CSP expected to act on a warrant when the best place to place the intercept is physically located in the United States where wire-tapping legislation is rather different? If the government sees this as a design issue ("you should not design your networks that way") then this is a considerable imposition on our freedom to develop our business in an effective manner [Hall *et al.* 1999; see also Parr 1999; Emery 1999; Sutter 2001].

7.4.3. The Cultural Shift of Deregulation.

In addition to the legislative shift, which resulted from deregulation, UK interviewees indicated an equally significant –yet largely implicit– cultural shift which characterises some of the underlying qualitative differences between former state monopolies and the new, private sector CSPs. Both BT[47] and independent CSP interviewees appear to recognise the special status that BT enjoys in the industry's relationship with law enforcement:

> I think it's [...] different in a lot of ways, because British Telecom have their own investigations unit and investigation arm, which [...] means that they can talk to [law enforcement] in the same sort of level and they have a lot more powers [...] from their [...] sort of [ex-]Post Office days. And they do tend to sort of take a lot more ex-police and ex-[secret] services anyway. So they talk the same language. And [it's] also their size –[...] they have a lot more power. With ourselves, [...] we have to do it by friendly social beings [Fraud Control and Revenue Assurance Manager of large UK wireless communications company, Int04:224-231];

> [t]he Post Office has been assisting in the interception of mail and then telephone calls [...] since the 17th century. So, if you like, the [...] culture of co-operation with the government and the [...] maintenance of whole structures within [...] BT that are concerned with the interception and maintaining the secrecy and security over interception operations, has been there organically, sort of stripped through the organisation. And that cuts both ways; I mean, not only does it mean that BT are very efficient in doing that and they have specially-trained [...] engineers who do that [...], but that the government trusts them to do that job [Bowden 2000:555-563];

[47] "[T]here's a gap [...] between ourselves [and new carriers]. BT [has been] carrying out interception on voice networks –POT voice networks– for years; there are established processes and procedures and established cost-recovery mechanisms, so that we can recover part of our reasonable costs" (British Telecom Regulation Affairs Officer, Int11:118-121; see also Int07:251-255).

> [there is considerable] difference between different companies and their attitude to what extent their organisation is part of the law enforcement process or [...] to what extent their organisation is incorporated to law enforcement. I think the older the institution is and the more established it is, the more it feels that [...] it's part of the [law enforcement] establishment [Regulation Officer and law enforcement liaison of large ISP association, Int10:222-227].

In contrast, the institutional interface between law enforcement and newer CSPs remains largely unstructured and unformed, something that is typically reflected in their cultural structures:

> Internet service providers [ha]ve only sprung up in the past 7 [or] 8 years. Before that there wasn't such a thing as an independent service provider. [C]ulturally they have few [...] commonalties with law enforcement [...]. Whether the[ir] relationship [with law enforcement] can ever be quite as sort of cosy and seamless as it has been with BT, I doubt [Bowden 2000:563-566; 602-603];

> there is [...] an agreement [between BT and law enforcement] that there's [...] a need for interception, which is legitimate –a need to meet certain objectives in society. Where there's some more doubt and less understanding is [...] typically with ISPs –the small operators– who have not been involved in the process at all before [British Telecom Regulation Affairs Officer, Int11:80-83].

Law enforcement officials appear also to be recognising this cultural shift and, prior to RIPA's enactment, consistently called for a change in the legal regime of CI in order to limit or even eliminate the potential harm to state-sponsored CI by uncooperative CSPs[48]:

> [w]hilst we currently enjoy a level of co-operation from most communications service providers unparalleled in Europe and the rest of the world, this cannot be guaranteed and, as such, th[e government's] proposal to introduce a statutory requirement appears prudent [Sims 1999; see also Veigas 1999; Maddison 1999].

The situation appears to be rather similar across the Atlantic, with older carriers revealing a sense of reassurance about their historical arrangements of facilitating state-sponsored CI, younger carriers refusing to honour CI requests in the absence of sufficient documentation, and law enforcement reminiscing the "good old days" (Int19:723ff) of the AT&T monopoly:

> BellSouth [...] have been doing intercepts longer than I have been alive [and] are fully aware of the security concerns. [As an] incumbent carrier [BellSouth] have had a long-standing relationship –a long-standing history of co-operation– [with law enforcement] and the younger carriers haven't even thought of what they have to do. They're [...] not as [...] mature a company as we are. I am sure that when they are presented with a court order [...] it's a new thing to them and they're not used to dealing with that sort of thing [CALEA Compliance Attorney, BellSouth USA, Int20:321-327];
>
> [our relationship with law enforcement] is just like anything, you know, you build rapport and then you have a certain comfort level at some stage in the relationship [CALEA Project Manager of a large US telecommunications carrier, Int21:155-156];
>
> [we have] policies and procedures on how to handle a request [...] for a surveillance and [...] we're going to stop them at the door and say "hey, this is what you need to have and this is what we're going to do. And if you don't have it you 'ain't gonna get it'!". Bottom line [Technical Director of a national telecommunications association representing more than 500 small-size CSPs, Int17:229-233];
> before the break up, [...] the phone company [...] was totally responsible. They'd give you that information within as quick and orderly fashion as possible [Technical Unit Chief, Emergency Communications Unit, Int13:123-126];
>
> the industry, 20 years ago, was half a dozen companies. And I knew all of the players and the security people. And they had a very tight ship as far as the security of the information; and it was a [...] very closed family, this relationship between law enforcement and telecom[munication]s. Not so any more. Telecom carriers in particular are springing up every day. New people, companies that have never even thought about the intercept angle that they're going to be involved in. So, in that respect, there are a lot of new players many of whom we do not have close working relationships with and they may not share [our] main concerns about keeping the information secure as we would or other carriers [would]. I know that sounds goofy but I would view [...] and characterise [the pre-break up era] as the 'good old days'. It was easier, it was old-hat, [...] everybody had done it. It was pretty easy and straight-forward [FBI Special Agent, CALEA Implementation Section, Int19:681-689, 723-725].

7.4.4. The Financial Shift of Deregulation.

Apart from encouraging a variety of cultural shifts within the telecommunications industry, deregulation also entailed financial implications for carriers. The degree of competition escalated, transforming the UK and US telecommunications markets into symbols of antagonistic liberal market ideology in late 20th century state capitalism.

---

[48] During the IOCA consultation, Demon Internet warned the UK government that "[i]n the relatively near future ISPs are likely to insist that the police always have a warrant before data can be made available to them" (Hall *et al.* 1999; see also Challenor, undated).

Consequently, law enforcement's CI needs were subsequently degraded into low-priority concerns by an industry that was simply too busy being competitive:

> the newer, brasher tel[e]co[mmunication]s [carriers a]re rushed off their feet just doing their day job and [to] anybody who comes along asking for something else they're going to say "oh, heavens above, I'm far too busy, go away! I'm trying to run a business here" [Regulation Officer and law enforcement liaison of large ISP association, Int10:480-484];
>
> [carriers had] heard what law enforcement's needs [and] requirements were –they'd had that in writing– and, at a technical level, they understood it. But they were not willing to make any modifications to their equipment, because [...] they had their most talented engineers working on features and modifications to the equipment that would make them money. Why work on this non-profit making feature? As important as it was to us it was certainly [not] bringing in anything for them [FBI Special Agent, CALEA Implementation Section, Int19:168-174];
>
> law enforcement are looking to us to volunteer to put CALEA technology in everywhere at our own cost [...]. But in a competitive environment we can't give stuff away, you know, we've got to operate to make a profit [CALEA Project Manager of a large US telecommunications carrier, Int21:96-98].

Industry representatives have been particularly vocal about what they perceive to be a direct and threatening link between optimising RIPA and CALEA modifications[49], on the one hand, and maintaining the financial prosperity of their business, on the other:

> [in implementing IOCA] the government runs a very serious risk of damaging our ability to compete [...]. Any proposal that degrades the level of service that we can offer to our customers will affect our position in a highly competitive worldwide market [Hall *et al.* 1999; see also Perry 1999; Anon 1999d];
>
> [f]orcing industry to become CALEA compliant in under two years would not serve "the policy of the United States to encourage the provision of new technologies and services to the public", as enormous amounts of time and engineering manpower –otherwise employed in the provision of such desirable technologies to the public– would have to be dedicated to an accelerated implementation of CALEA [Baker *et al.* 1998].

Rather predictably, therefore, concerns relating to financial compensation by government for CALEA and RIPA network modifications crown the industry's list of concerns over the two pieces of legislation, far surpassing privacy or capacity issues (Int01:1997-199,

[49] ISPA council member Tim Snape reportedly characterised RIPA modifications as an "intolerable commercial burden" (ctd in Delio 2001).

210-214; 359-361; Int19:553-562; Evans 1999)[50]:

> [financial compensation] is an overhead. What's in [assistance to law enforcement] for any organisation? You're a good corporate citizen, you're a good member of society, if you like, but it's not actually adding to the bottom line [...]. We are looking at [RIPA] for commercial reasons, actually, rather than particularly moral reasons [British Telecom Regulation Affairs Officer, Int11:63, 106-108].

> I think that the breadth and the scope of our putting the CALEA functionality in our network is going to depend upon the extent to which we can expect reimbursement of our costs. And so, [...] the extent [to which] the government can [...] identify additional moneys in other areas of law enforcement –that will help facilitate CALEA [CALEA Project Manager of a large US telecommunications carrier, Int21:173-175].

Increasing sensitivity over public relations –arguably a side effect of customer-driven deregulated industries– was also influential over the industry's overall view of CALEA and RIPA, although apparently it often had contrasting effects:

> you see, it's not [...] that there may be [a] more civil libertarian sort of attitude in the management [of certain carriers] or whatever. It's just the fact [that], if they get things like that wrong, they might end up being sued by a customer for damages [.... A]nd if it leaked out that a particular ISP was over-co-operative with the police on interceptions, a lot of the customers would say "I'm sorry, we're going to find another ISP" [Regulation Officer and law enforcement liaison of large UK ISP association, Int10:583-589];

> [carriers] were very much [thinking]: "[what would happen] if we sort of had a PR [(public relations)]scandal, if something like this happened and our network, our company, our equipment was identified as the problem by which the little girl was kidnapped because law enforcement couldn't get her contact information"? They were very scared of that. [A]nd that was the only motivator that I saw. I did not see any altruistic motivation by the carrier or the manufacturer to take [...] a stand and do this because it was the right thing to do. I'd love to say that [FBI Special Agent, CALEA Implementation Section, Int19:183-192; see also Int13:140-142].

[50] "[I]n the wireline world [carriers] go to these commissions and make a plea to modify their rate structure to recoup these [CALEA modification] costs from their subscribers. No carrier wants to do that. Who wants to raise their rates? Who wants to put on a 'wiretap tax'? It would kill them. So that's not really a viable option for many carriers. Well, wireless people, they're not in any better position. If you look in today's paper you'll see them begging you, giving you minutes or extra time for a dollar less, everybody's cutting each other's prices. Well, the last thing they want to do is buy more expensive equipment to provide you with that same service. They want to do just the opposite. So, [CALEA] capability equates to cash. The less capabilities they provide, the more cash they're able to provide their stockholders" (Int19:553-562). "The first thing the phone company says when you meet with them is "will we have to charge the customer under the [CALEA] contract?" (Int13:11-12).

7.5.0. Negotiating Over Digital CI.

Any attempt to outline the negotiations that preceded and followed the creation and introduction of RIPA and CALEA should commence by attesting to the element of secrecy, which has inevitably withheld large portions of the debate from researchers and non-security-cleared observers.

7.5.1. US: "If I Could Only Tell You What I Know...".

Evidently, to those who work within US governmental organisations, large segments of the debate over CALEA are seen as a matter of the citizens trusting their elected representatives to handle security issues that are too sensitive to be publicly negotiated. While helping to erect and maintain near-impenetrable security walls around some of the more detailed aspects of digital CI, it is indeed not hard to imagine how such convictions tend to eliminate debate on the issue before it even commences. Asked at a press conference whether US citizens should entrust the nation's intelligence services in having a say in the design of the digital telecommunications infrastructure, Michael Nelson, who was at the time the US government's advisor on the National Information Infrastructure, laconically replied: "[i]f only I could tell you what I know, you'd feel the same way I do" (Barlow 1994). Another sympathiser of law enforcement's demands has remarked that

> [u]nfortunately, it is not possible for most of us to be fully informed of the national security implications of [these matters]. For very legitimate reasons, these cannot be fully discussed and debated in a public forum. It is even difficult to talk about the full implications [...] on law enforcement. This is why it is important that the President and Vice President be fully informed on all the issues and for the decisions to be made at that level [Denning 1994].

This opinion largely reflects attitudes on CI among the nation's security and intelligence establishment. In a lecture at MIT, former Director of the NSA, Deputy Director of the CIA and Director of Naval Intelligence Admiral Bobby Inman admitted that, had the Agency had its way, the current policy debate on digital CI would not have "over-spilled" onto the public arena (ctd in Lethin 1995). A few months earlier, Federal Agent Barry Smith, a member of the FBI's Congressional Affairs Office, had remarked that, if a solution to the digital CI problem was eventually reached, the FBI would avoid even publishing a press release on it: "it will be done quietly, with no media fanfare", Smith admitted (Meeks 1994).

In reality, despite the alleged "over-spilling" of the CI debate, few details are known in regards to the negotiations between law enforcement and industry[51], while even less information is available about negotiations between law enforcement and government officials prior to the introduction of CALEA. Throughout the 1990s, numerous closed briefing sessions were conducted between members of the US Congress and members of US law enforcement agencies, including FBI Director Louis J. Freeh[52]. In general, the vast majority of governmental, law enforcement and industry representatives who take part in CALEA negotiations require security clearances and usually receive a *Regulations and Procedures* memo warning them not to reveal classified information imparted to them, not to make written notes of classified discussions, and to report to the authorities any attempt to obtain classified information from them (McCullagh 1998).

7.5.2. UK: Secrecy as a Precondition for Debate.

Regrettably from the standpoint of political research, large segments of the negotiation process that eventually led to the introduction of RIPA –probably the most crucial, cynics would argue– have been clandestine. The initial interactions between law enforcement and industry representatives, in which a solution based on consensus, rather than on legislation, was pursued, were conducted in secret[53]. According to Yaman Akdeniaz, whose organisation, Cyber Rights & Cyber Liberties UK, exposed the existence of the initial set of meetings,

> we thought it was secret –which it was. They called it an "internal document" [but] I think it was secret. It's pretty safe to say that was secret, because once all interested parties are not included in these meetings or negotiations, then there is secrecy [Int01:376-378, 24-27; see also HCTISC 1999].

Following the initial introduction of IOCA, when the negotiation process over RIPA assumed a less clandestine format, a certain degree of secrecy remained a foremost precondition for the debate, and it was apparently respected by all participants, including civil liberties groups:

> [w]hat generally happens after several meetings [...] is [that] some sort of trust develops [and] a dialogue of some kind is going to be possible

[51] See n37 above.
[52] One such session that raised considerable reactions by non-governmental observers was held on 26 June 1997 by the House International Relations Committee (Anon 1998c; see also Leahy 1995; Berman & Dempsey 1996).
[53] See n15 above.

> without necessarily everything that either side says being [...] noted down –i.e. put on the Internet or trumpeted to newspapers [Bowden 2000:296-300];

> we [all] respect [each] other's confidence and certain information handed over. I mean, some of the information is clearly public. So, for example, when this civil servant gives me –as he did– [...] a copy of this and says "here you are, have a copy of the Smith Report and read it" [...], he will give me a copy of this two days before it's published. We [...] went to the Home Office and they said "look, here is a copy of it, please don't show it to anybody, but there you are". So [...] the relationship of trust and good understanding may well be coming from why we've been invited to the meeting –what we' re supposed to do, how we're supposed to react [Regulation Officer and law enforcement liaison of large ISP association, Int10:169-177].

To a large extent, the secrecy that permeated negotiations over RIPA was justified by the sensitive nature of the subject under negotiation[54]:

> the whole process has been up to now fairly restricted to [...] telecom[munication]s operators and [in] the existing IOCA it's to be restricted [...] to those. So, [it's] been quite a homogenous population of people –and a small population– who have been required to intercept communications on behalf of law enforcement authorities. So, those people have had a clear view, to start with, of why it's been required and understood the controls that were applied, which certainly previously have not been particularly visible outside of this, sort of, fairly exclusive club [...]. The number of people who know the detailed process –the less they are the better, really. [I]t is a difficult issue [...] simply because previously [...] it's been [...] a very specialist area, which, [...]by its very nature, you tend to need to keep secure. You don't want to [...] talk about it too much, because it's counterproductive. [British Telecom Regulation Affairs Officer, Int11:20-26, 89-92, 125-126].

Yet, UK law enforcement interviewees claimed that even the acknowledgement by the law enforcement and intelligence community of lines of communication and negotiation with carriers marks an astounding shift in policy, namely the acknowledgement of a relationship that, in previous years, would have hardly been publicly admitted, let alone documented:

[54] "There's no clear solution [.... O]n the one hand you do have the fact that large parts of security and intelligence policy can't be conducted anything less than secretly –it can't be in the public arena. But on the other hand, where there is some major policy area of controversy, you do appear to get judgements taken by Ministers at what seems often like a crass level. I mean, it's always very dangerous saying that, but what one can say for certain is that the arguments which Ministers roll out in public do appear to be crass. They overlook very obvious issues [...] and [...] they [...] don't hang together logically. Now, of course, it's possible that [...] there [...] is some backdrop which only the security services and the Minister in fact know and that the reasons that the arguments put up are so transparently weak is because the real arguments cannot be put forward in public. And that's always a possibility. But the evidence in this area of interception is not reassuring" (Bowden 2000:257-269).

> I mean, you've only got to go to the NCIS web site to see how open that organisation is. And certainly, I mean, you know, in the timeframe of the last two to three years, increasingly more open. [P]rior to that, no. Prior to that [contact would take place] behind close doors. And you wouldn't even discuss it –you wouldn't even [...] admit its existence half the time [Former Special Branch Officer, Int12:451-455];

> I can tell you for a fact [that] some [of the] official documents [on the RIPA that are] circulating in public shock even law enforcement [members] themselves –some of the older members. I'm sure they're shocked to see no "restricted" [labels] on these documents. I am sure they are, because I am too. But times [are] changing [...] rapidly [Former Special Branch Communications Intelligence Officer, Int02:319-321, 344-345].

7.5.3. Law Enforcement Disunited.

Much of the analysis of the RIPA and CALEA debate has tended to assume that the negotiations over the two pieces of legislation were primarily conducted between two groups of united and cohesive actors, namely the law enforcement and intelligence establishment, on the one side, and the CSP community, on the other (Sutter 2001). A more thorough examination, however, shows that the precise nature of these two groups tends to be characterised by the unequal and problematic alignment of disparate parties in pursuit of common interests at best, or by the patchy amalgamation of competing interests at worst. The UK law enforcement bloc is a particularly interesting example of this. Although official documents appear to show uniformity of opinion over RIPA among ACPO, HM Customs and Excise and the various intelligence agencies, including the Security Service and GCHQ (Gaspar 2000:§1.1.1), there are reasons to believe that this uniformity is, in fact, not representative of reality. According to one interviewee:

> [e]ven though the ACPO people are the most noticeable law enforcement people out there in defence of [the] RIP[A, the] National Criminal Intelligence [Service is] the real engine behind the campaign [...]. You have got to remember that ACPO is made up of older policemen [sic] – old school police [officers]– who don't really understand much about electronic interception. I mean, very few Police Forces out there make heavy use of interception in investigations: Scotland Yard, Greater Manchester, West Midlands, maybe Glasgow and Leeds [...] and that's [...] about it, really. So [ACPO] would have had limited knowledge about the [CI] problems that came up [...]. Maybe some people in CID did encounter some [problems] –in fact, I am sure they did– but they would have had no way of knowing why the[se problems] were appearing. So the leads came from NCIS and [...] GCHQ and were eventually streamed all the way down to ACPO [...]. And, frankly, [...] most of the ACPO people are not particularly bothered about [the]

> RIP[A], because very few of them will ever use it. NCIS, on the other hand, are very up-front about some of the more technical issues [in the Act], such as encryption or data retention, etc, because they will be the ones that will primarily use them –they and Government Communications [Headquarters] [Former Special Branch Officer, Int02:411-413, 417-430].

Some of these differences of opinion, which unavoidably exist with the law enforcement RIPA lobby, and perhaps within ACPO itself, can be traced to the written responses to the Home Office by law enforcement officers responding to the IOCA consultation. One respondent called for a more open discussion on CI, disputing the official law enforcement argument that detailed public discussion over the issue would benefit criminals:

> I do not agree entirely with the argument that exposure of interception capabilities will educate criminals as those involved in crime at this level are already well aware of what our capabilities are [Stoddart 1999].

Additionally, the same respondent rejected CI authorisation protection from the NCIS, requesting that local police forces authorise their own CI requests without the need to resort to NCIS interception experts (ibid.). Another respondent varied from the NCIS' view of the ECHR as a threat to UK law enforcement's interception capabilities and stressed that

> [c]ompliance with ECHR is of paramount importance and this must be stressed throughout the consultation process [Grey 1999; see also White 1999].

Two other respondents expressed the view that CI requests to CSPs should be kept at an absolute minimum, and be reserved for cases of serious criminal activity with ample consideration given to the intrusion that the practice of CI can represent to the private lives of citizens:

> [c]ommunications service providers cannot be expected to supply information to the police for every case, no matter how minor [Todd 1999];

> [t]here are obvious concerns as to the consequent level of intrusion, which [CI] represents and I would suggest that this dictates the minimum authority level to be at Detective Superintendent Rank (as currently exists in my Force). This should provide a safeguard to those concerned with the potential for abuse and reassurance to the data providers that their interests are being considered [.... T]he principle must be that we are "whiter than white" and must be able to evidence that fact [White 1999].

In the US, the federalised character of the law enforcement community means that the law enforcement CALEA lobby has been even more fragmented than the UK's law enforcement lobby. Almost a dozen[55] federal bodies are actively involved in CALEA lobbying and implementation, and many of these organisations are often in disagreement about the specifics, much less the general direction, of the legislation and its implementation:

> when the [J-STD-025 or] J-Standard came out, in December of [19]97, [things] turned really sour. I mean [...], it was almost like we had never even talked to the industry –they [...] had just gone out and [...] done their own thing. We had [...] to go up to Chantilly[, VA, and] it was just...simply unpleasant. Allegations were flying across the room; some [people] questioned the FBI's handling of this whole CALEA operation. There were two [representatives] there from the Secret Service and they [...] eventually [...] got up and left the meeting. It was that bad [First Class Sergeant, Communications Officer, United States Special Forces, Int14:112-113, 115-122];

> [n]ow, [...] I know that [the FBI] have formed a law enforcement group [or] consortium [.... W]hen dealing with them on some of the issues [...] they seem to be saying "OK, we agree with you" and then they would disappear and come back and say "oh, we can't agree with you". Because they would get together with th[e] DIA and...and the CIA [...] up there in New York City [...] with a whole bunch of law enforcement people and [...] go through this [USTA CALEA lobbyist and point person, Int16:260-266].

Virtually none of the US interviewees who were actively engaged in CALEA negotiations were prepared to interpret law enforcement's CALEA lobby as a solid and uniformed bloc of actors[56]. It was generally agreed that the FBI has been the lobby's primary representative during the negotiations (Int20:29-30; Int16:267-270) but it was

---

[55] They include the US Air Force Office of Special Investigations (USAFOSI), the US Secret Service, the US Marshals Service, the US Customs Service, the US Postal Service, the US Bureau of Alcohol, Tobacco and Firearms (USBATF), the US Drug Enforcement Administration (USDEA), the US Department of Defence (USDoD), the United States Food & Drug Administration (USFDA), the US Internal Revenue Service (USIRS) and, of course, the FBI (see Yarbrough 2000).

[56] "To do a surveillance [local law enforcement agencies often] have to contact the FBI in order for them to get the information [on their behalf]. And they don't like that. People don't like working with the FBI, because they find that the FBI comes into their jurisdiction and they kind of take over. And then you start getting into turf battles" (Int16:272-276). "[T]he distinction between the way law enforcement is tiered here in the States [means that] we have a lot of turf battles. And everybody guards their territory rigorously and they don't like anybody exceeding over into their [...] territory. And we constantly [see] that in the federal agencies. You've got [...] the Customs, DCI [(Director of Central Intelligence)], FCC, [...] Secret Service, [USB]ATF [...] and all of them go up against the [Federal] Bureau [of Investigation]. Because the Bureau has [...], I would say, almost omnipotent authority [...]. Their jurisdiction overlaps into a lot of all the other [agencies'] jurisdictions, even though the others have primary [authority] in certain areas [...]. But that's always been like this in law enforcement. There's always been conflict. When you cross turf [it's like] "[...] that's my boundary, don't cross over. If you do [it] you[...]'ll get my wrath" (Int21:76-87).

noted that this was not decided overnight:

> you've got a bunch of different federal agencies that have surveillance authority and [...] it took a while, I think, for the FBI to be viewed as the lead agency on it. It just took a while for consensus to develop [CALEA Compliance Attorney, BellSouth USA, Int20:199-201].

A particularly deep schism that runs through law enforcement's CALEA lobby is that between Federal and large metropolitan state and local law enforcement institutions, on the one side, and small-sized or rural police departments, on the other. According to FBI's own sources, less than a third of US states are actively consulted and represented in law enforcement's CALEA lobbying and implementation bloc (Yarbrough 2000). An FBI interviewee asserted that state and local law enforcement officials are often not even aware of CALEA and its implications:

> [are] state and locals [...] aware of CALEA? Well, some are not. Many are. Some are not aware of CALEA's provisions and the fact that [...] times are changing as far as the way intercepts are done. I will not gloss this over. There is a surprising amount of ignorance sometimes [that] I see with state and locals about CALEA and how it's going to dramatically effect [...] the equipment that they are going to need, the expertise that they're going to have to have on board and the paths by which [...] they are going to do intercepts in the future. They do not have a firm grasp [FBI Special Agent, CALEA Implementation Section, Int19:327-333].

A long-time industry participant in CALEA negotiations with law enforcement confirmed the situation:

> [w]hat's very important to understand is that this is a Federal Bureau of Investigation effort to push this through. Most of our companies who go out to talk to local law enforcement are coming back to us [...] saying they have no clue what this is all about. The local [...] police departments, the local sheriff's department, the county sheriff's department, even to the point of the state police have no idea what this is about. When you look at the law [...] it says "law enforcement", and that includes all of them, all levels of law enforcement, and yet they have not done the job and brought it down to all the levels of law enforcement as to what this is all about [Technical Director of a national telecommunications association representing more than 500 member companies, Int17:219-226].

The official reason provided for this dichotomy is that the vast majority of state-sponsored CI requests are issued in large metropolitan areas and, therefore, this particular investigative tool does not necessarily concern small- or medium-sized police

forces across the country[57]. The actual reasons, however, appear to be quite different, and have to do with the close nature of the relationship between smaller law enforcement agencies and smaller communication service providers. Namely, the personal element that characterises such relationships in smaller communities means that a considerable number of CI requests by law enforcement are authorised on face value by over-familiar carrier executives and employees, rather than by the courts[58]. Consequently, smaller law enforcement agencies have a negative view of the more structured CI request format introduced by CALEA, which they perceive to be a threat to their usual –and effective– process of conducting CI:

> people are afraid [...] that when you force smaller carriers to build [...] surveillance capacity into their switches, then the small carriers are going to have to charge [...] for the service, [in order] to get their money back – which indeed they will. And so, what you have here is that [local police] forces [operating] on small budgets fear that they're not going to be able to afford to wiretap any more. They're going to have to get charged for it and the whole request will have to be routed through formal channels [by the carrier] [First Class Sergeant, Communications Officer, United States Special Forces, Int14:146-151; see also Int16:270-272, Brown 2001].

7.5.4. The Industry Mosaic.

If the law enforcement bloc in the UK and the US has simply been rather disunited over CALEA or RIPA, then it can safely be asserted that any reference to 'an industry bloc' in these negotiations is highly misleading. This applies particularly to the UK, where the relatively recent appearance of RIPA has yet to allow the formation of a reasonably cohesive industry lobby. The US industry landscape, in regards to CALEA, is also rather fragmented, primarily in accordance with the market positioning of individual corporate actors.

Broadly speaking, experienced RIPA and CALEA industry negotiators were keen to stress that "the telecommunications industry is not a single object" (Int10:52), but rather a "complex body" (Int12:128), various parts of which are "focused on totally different disciplines" (ibid.:129) and were essentially slow in achieving even basic consensus over

[57] "Now, where are [CI requests issued] the most? [I]n New York City, [NY,] in Washington, DC, and the major metropolitan areas. And that's not always the voice of [...] state and local law enforcement. Knoxville, Tennessee, probably doesn't have, or ever has had, [...] an instance where they needed to intercept a satellite telephone. But New York has and the fed[eral agencie]s have too, particularly as we are involved in international criminal conspiracies or across state lines, too" (Int19:316-323).
[58] See section 7.6.0, further on.

digital CI provisions (Int20:183, 183-195). One major reason for this fragmentation is the culture of extreme competitiveness and antagonism that characterises the industry, which was briefly mentioned earlier[59]. One UK carrier representative characteristically described the way in which highly competitive relations between CSPs impacted on the industry's IOCA negotiations with the British government:

> when you [...] have these meetings [with the government] it's not always on a one-to-one basis. I think in an informal [one-to-one] meeting [with the government] we'd always [give detailed information]. In the [...] formal briefings that I've been [to] in the Home Office, when you're there with Vodafone, when you're there with Orange [...] or BT, you don't tend to sort of say "well, we are developing this service and you might not be able to intercept it, because of this, this and this". Of course the other guys are going to realise what we have in mind and are going to say "oh yes, that service, how far are you away from launching that? Alright!". So commercial implementation ties you and you just can't reveal too much, but informally we would give [the government all] sorts of ideas [Fraud Control and Revenue Assurance Manager of a large UK wireless communications company, Int04:282-290].

Another interviewee, working for TUFF –arguably the UK industry's most active point of interface with law enforcement– disclosed that separate segments of the UK telecommunications industry operated in almost complete isolation from one another during the IOCA and RIPA consultation period: "telecom[munication]s industries didn't even talk to telecom[munication]s industries!" (Int12:357-358).

In the US, similar illustrations of the industry's fragmentation were provided by an FBI interviewee, who held the industry's lack of policy cohesiveness directly responsible for the delay in the standardisation and eventual implementation of CALEA's guidelines:

> [u]nfortunately, the ECSPC[60] meetings weren't very productive, mainly because there were competing interests in the room –carriers, manufacturers– all of which were competing against each other, none of which wanted to provide much information as to (a) what information is floating around in the network that [...] may be accessible to law enforcement, [and (b)] how that information could be retrieved. [This was] because they did not want that information revealed to their competitors. And that was a real wakeup call for law enforcement. We had no idea of [...] the cutthroat competitive nature of the industry. And, what appeared to be relatively innocuous information about a telecom[munication] carriers' switch, was guarded zealously by the manufacturer –and the carrier, for that matter– and they were [...] very reluctant to provide us [with the] number of switches, the features on

[59] See section 7.4.4 above.
[60] See section 7.4.0 above.

> those switches, the generic modules on those switches –basically where we would do our intercept [.... N]othing productive happens when you bring in competitors to a [...] room. [We] got nowhere [by] bringing them together, so we [had to] meet every day with them individually. We had calls with them individually every day about CALEA [...]. And that [...] in itself slowed things down, because you had an assortment of interests in a room –say 60 people, a 'who is who' of the telecom[munications] industry– trying to agree on how an intercept would be done. They had a very difficult time agreeing on how anything was done [FBI Special Agent, CALEA Implementation Section, Int19:60-72, 97-100, 795-799].

In the US, a clearly detectable line dividing industry is that between switch or network owners –namely the carriers– and switch manufacturers. In a manner comparable to the *Operator Action* scheme[61], which was proposed by industry members in 1998, numerous switch manufacturers sided with law enforcement's digital CI plans after sensing CALEA's potential for large-scale government-appointed contracts[62]:

> [t]here were some [switch manufacturers] that, for market reasons, decided to be leaders in developing or implementing the CALEA standard and in one case doing it before the standard was complete. [They did this] because they saw a market niche [...] and they foresaw – and correctly so– [...] a demand for CALEA-compliant switching equipment. So [...] they were definitely out of the chute first, making mod[ification]s to their equipment so that they could be there by the market with CALEA-compliant switches [FBI Special Agent, CALEA Implementation Section, Int19:192-198];

> [m]ost manufacturers long ago began designing and developing solutions even to some interception capabilities excluded from the standard. In fact, several manufacturers are well along the way. Moreover, a number of the manufacturers have developed many of the needed CALEA solutions in their switching platforms in order to meet CALEA-like solutions required of them by statute or otherwise by law enforcement or national security entities in a number of foreign countries [Morris 1998].

While this thesis is being finalised, ongoing CALEA negotiations in the US have yet to

[61] *Operator Action*, also known as *Private Doorbell* technology, was a slight variation from key escrow; instead of a third party holding a decryption key –as was the case with key escrow– *Operator Action* allows the interceptor to access and decrypt encrypted messages at the network's router switch. The scheme, which was approved by the FBI and the NSA, was proposed by 12 hardware and software network manufacturers, which included Cisco, Inc., and Bay Networks (see Mosquera 1998; Mills 1998; Appleby 1995; McCullagh 1998; Mills 1998).

[62] In the words of one US switch manufacturing insider, "the government is increasingly looking towards the industry for software support solutions and assistance in the exploitation and analysis of intelligence information. There's a public/private partnership being formed out there and it's becoming an integral part of [...] the provision of all-source intelligence infrastructure" (Mahler, undated).

produce a mutually accepted technical standard for digital CI. Nevertheless, Cisco and Nortel are already in the process of producing intercept-friendly network switches (see section 6.3.1) for both US and UK markets (Int11:132-134), while Lucent, AG Communications, Siemens and Bell Energis have either completed or are in the process of finalising their CALEA-compliant switching products (Hildebrand 2000; Heupel 1999; Anon 1998d).

The telecommunications industry in both the US and UK digital CI debate is also polarised between the older, wealthier carriers, on the one side, and the newer corporate up-starts, on the other. On both sides of the Atlantic, concerned industry participants in the digital CI debate have expressed concern over the logistical costs that would be associated with the implementation of RIPA or CALEA. The requirement of employing staff as points of contact with law enforcement, who would have to be available to the latter 24 hours a day, 365 days a year, may prove particularly costly (Int18:169-172; Perry 1999; Morris 1998; Auble & Bender 2000), while the labour costs associated with retracing, retrieving and filtering data requested by law enforcement is described as potentially "massive" (Int08:370-373):

> [according to t]he way the [RIP] Bill is written at the moment, law enforcement –which could include [...] minor officials– could actually ask for the most obscure types of data, which [...] service providers are currently gathering. And there is nothing in there that says they couldn't do that. So, they could come along and say "we'd like to [...] have a list of all the people with a 'z' in their name, who emailed all the people with an 'x' in their name last Thursday afternoon". And that'd just be [...] communications data. The [...] service provider would say, "well, for heaven's sake, I don't collect that, you know, I don't know that!". And they'll say "well, I'm sorry it says [in] section 42" or whatever "of the Bill [that] I can ask for anything I want and you've got to give it to me". And they'll just sort of stand there until something happens[. The] service provider would have to comply [Regulation Officer and law enforcement liaison of large ISP association, Int10:421-431; see also Int08:358-362, 374-378, Stewart 1999; de Stempel 2001].

There is no evidence to suggest that the wealthier, more profitable telecommunications corporations are in any major way concerned about logistical costs associated with the above prospects (Int04:299-301; Int17:71-75; Int12:525-532; Int07:11-16; Int01:466-468; HCTISC 2000), which they describe as "marginal" (Int07:10):

> BT, being a very large operator, [...] are already carrying probably too much machinery to deal with [CI]. And [...] there's probably room for

efficiencies [Int07:33-35][63].

There are fears among smaller carriers, however, that the imposition of such logistical costs on them by CI legislation would gradually turn them into a "law enforcement resource" (Bourne 2001), thus rendering them increasingly uneconomical:

> [s]maller [carrier] businesses are concerned about precisely what will be required of them [by the RIP]. For some, the requirement to invest in 'reasonable' interception facilities could mean the difference between profit and loss in the critical early stages of business operation [Anon 1999e; see also Int11:83-87, 100-106; Int07:32-45, 61-62; Perry 1999; Hall *et al.* 1999];

> [large carriers] have such tremendous resources, whereas smaller companies don't have the resources [...]. If you take [CALEA's requirements], those are things far beyond the capabilities of the small companies to [...] deal with [...]. All of the networking and the aggregation of [...] the [...] data redistribution and the single point [of contact] that's just [...] a level way above what these small companies that we represent would ever be capable of doing. So, [...] there's surely a problem with small companies having this imposed on them for [...] no reason [Technical Director of a national telecommunications association representing more than 500 small-sized member companies, Int17:77-84; see also Int18:154-157; McHugh & Cordwell 2000; Anon 1997a].

During the IOCA/RIPA negotiations in the UK, ISPs emerged as an exceptionally vocal segment of the smaller-sized CSP community (Lansman 2000). The reasons for this have primarily to do with the fact the vast majority of the more than 300 ISPs who currently offer services in the UK are operating on minuscule budges, a phenomenon that has given rise to what industry insiders often refer to as the 'mom 'n pop' ISPs:

> [RIPA regulations are] OK for us, because we run a 24-hour-7 shift [...]. But virtual ISPs have been known to use auto-pilot and go to holidays to[, say,] the Mediterranean for two weeks, and [there's usually] only that one [person] that has got access to the [customers'] home phone numbers and the home addresses. [S]o, let's say [that] the police know that somebody dialled in from that number and the [...] virtual hosting ISP says "well, [...] that's a StirlingNet customer". Who the hell's StirlingNet? StirlingNet [finally ends up being] a bloke living in some council estate in Stirling. So, [the police] try to get onto them. The phone number's ringing out; [they] send the cop car around. The neighbour says he's on holiday. Dead end. Does the guy go to jail for not responding properly?

[63] The following –rarely publicised– information about BT's Security Department is particularly impressive and gives an idea of the size of the company's security and investigation budget: the Department consists of no less than five different sections: Directorate of Security & Investigation; Commercial Security Unit; Specialist Services Unit; Computer Emergency Response Team; and Investigation and Detection. The latter of these, which is based in Milton Keynes, employs more than 50 detectives from a variety of backgrounds, including police, military intelligence, Customs, Inland Revenue and the Department of Social Security (Bleep 1992; Anon 1994).

> That's the worry of RIP. These people are lucky if they have a sales office. Everything [is] outsourced [CEO of large UK Internet service provider, Int08:57,110-121].

Independent cost studies of the RIPA in the UK have estimated that, on average, ISPs will be required to facilitate approximately £20,000 to install RIPA-compliant interception technology and £10,000p.a. for maintenance and logistical costs (Clayton *et al.* 2000). Demon Internet, one of the nation's largest ISPs, calculated its RIPA-related costs to an amount equal to 15 per cent of its total revenue (Sutter 2001). ISP representatives have remarked that, if these estimations are indeed accurate, most of the UK's ISPs will be forced out of business (Int01:199-203; Snape 2000; Clayton *et al.* 2000; Anon 2000a).

7.5.5. Challenging RIPA: The Illusion of Negotiations.

Considering the degree of fragmentation within the UK telecommunications industry, it should not appear surprising that the latter's concerns over RIPA had a negligible impact on the Act's stipulations (Int01:290-291; Clayton *et al.* 2000). The overall feeling among UK industry interviewees was that they were unable to leave any considerable mark in the legislation[64]:

> [a]s far as the drafting process is concerned, [our legislative impact was] zilch [TUFF fraud and law enforcement liaison officer, Int12:161];

> from a Security Department point of view the consultation that [...] we had was adequate to tell [us] what was going to happen but there was no question of asking [us] what was going to happen [.... W]e're not making the law here –the government is. And they, you know, it's handed down to strategy to be made into tactics. [It's v]ery much top down, really. I mean, [...] I've [...] worked for BT since 1969 and [...] I've seen governments come along [...] and hunk lumps of [legislation]. [S]o it's not a question of [whether] you [...] trust them; it's a question of you just accept[ing] what they do [British Telecom Security Officer, Int07:52-58, 73-76; see also Int10:117-120, 130-132].

Additionally, UK CSPs are of the opinion that there was little genuine desire for fruitful negotiations behind the British government's call for the IOCA/RIPA consultation.

[64] According to one external observer, "certain leading ISPs have clearly tried to [...] work constructively on the RIPA problem. But, I think [...] that, to a large extent, their overtures have not been appreciated and, to some extent, rebuffed by the Home Office. I mean, it was only, really, [...] in [the] middle of last year that there was any contact that I'm aware of –significant technical contact– between the ISP industry and the Home Office. That's extraordinary. Because, clearly, this debate about encryption and the interception of communications in general has been running [...] for four or five years. It's simply extraordinary that up until then there was no direct contact between the

Rather, it is believed that the government was keen on creating the illusion of negotiations between industry and law enforcement, in an attempt to prevent over-zealous reactions by concerned CSPs:

> I mean, it doesn't really matter whether we trust the government or not, because we weren't [...] really negotiating with them [British Telecom Security Officer, Int07:68-70];
>
> the industry felt that this was being used as a sort of political selling job, to reassure Parliament at this time that, "yes, industry is working very closely with us, we've got a partnership" and all this lovely rhetoric. But, in fact, the ISP industry is not feeling particularly well consulted or particularly frequently consulted or, when it is consulted, that its message is being listened to [Bowden 2000:591-595];
>
> I believe they have already drafted the Bill. I believe the Bill was drafted and almost signed, sealed and delivered before someone had this afterthought saying "hang on, we've got to have a consultation process here".
>
> **Q:** Would you say that that was [done] to make sure that the government gets what the government wants?
>
> **A:** Correct. You know, it's [...] a marketing...I believe it is more [of] a marketing process than a genuine concern to say "well, have we got a right to [do] this, [do] that?". [O]ne has the feeling that it's not out of concern that the Bill might not meet our requirements. It's more out of concern that we would make a lot of noise against the Bill. And it's a certain amount of..."it is better", I suppose, "to have them on side where we can see and possibly influence what their reaction is going to be as opposed to not have them on side and then suddenly hit them with it and open the floodgates off". But I suspect the general view abroad is that we don't know how much of it is genuine consultation or how much of that is spin and marketing on the part of the government [TUFF fraud and law enforcement liaison officer, Int12:204-210, 248-253, 262-264; see also Int10:262-264; Int11:326-329].

7.5.6. Challenging RIPA: The Fraud Card.

Interviews unearthed a particularly interesting element in the RIPA negotiations between industry and law enforcement in the UK: namely, many of the carriers who were consulted in the debate requested –and could well have been promised, although there is no proof of that– that they receive increased assistance from law enforcement in combating telecommunications fraud in return for adopting a cooperative stance over RIPA. In recent years, telecommunications fraud, ranging from 'phone-phreaking' to

---

responsible department [or] the responsible officials and the industry. But that is so" (Bowden 2000:571-580).

cellular phone-cloning, and from network hacking to email spamming, has inflated dramatically, costing the wireless and wireline industry in excess of £400 million annually (Int09:322-324). Indeed, telecommunications fraud is today the UK industry's topmost financial and logistical problem (Roberts 1996). Admittedly, one of the reasons behind this dramatic increase has been the failure of UK law enforcement agencies to respond to telecommunications fraud with the same investigative urgency with which they tackle traditional criminal activity:

> I know from my own firm's experience [that] the situation [at the moment] is that one tends to try and get the crime reported in an area when one notes that there are at least one or two policemen that one might be able to have a conversation with who might understand the issue. We have been to local police stations to report a crime on the Internet and you do not get very far. By the time you have explained routing and domain names, the policeman has other things to do, obviously [Tim Pearson, ISPA Chairman, in HCTISC 1999; see also Int08:270-279; Int09:181-184]

> you're dealing with a [...] government instrumentality [and] with [...]limited resource and a massive remit. And so [...], I mean [to a police officer's ears] it's sounds like trying to convince [them] to come out and get a little old lady's cat down out of a tree [Fraud Control Manager of a large UK wireless carrier, Int06:180-184].

> I think there's been little movement in that direction –to get the police to understand our perspective. [T]here is a long, long way to go. If [...] we have a customer that is affected by a [telecommunications fraud] crime, we expect them to be able to go to their [...] local police station and report it and be taken seriously. And not to be rebuffed because [the police] don't understand it. Most of the times we have to talk our customers through a step of events that they need to do in order to be taken seriously [Fraud Control and Revenue Assurance Manager of a large UK wireless carrier, Int04:44-49].

The appearance of the RIP Bill, therefore, was seen by parts of the UK industry as an opportunity to push for the elevation of the status of telecommunications fraud in the eyes of law enforcement, in return for a co-operative attitude during law enforcement CI requests. In a 2000 presentation before a large group of law enforcement liaison officers of UK wireless and wireline carriers, the UK telecommunication's industry's designated Single Point of Contact under RIPA, Jack Wraith, characteristically described the industry's hopes for a new regime under RIPA:

> [up until now] law enforcement would not necessarily take telecom[munication]s crime, or telecom[munication]s fraud that seriously. It was almost like the blue collar-type crime –it doesn't affect

> anybody, nobody's heard, shrug of the shoulders and move on. That attitude is fast diminishing. And certainly now with single points of contact and, more recently, with accredited officers, they know that if they don't co-operate with our investigations on crime and help us they're not going to get the same in return. So, it is a certain amount of give-and-take in that respect [Wraith 2000].

Industry interviewees overwhelmingly reflected Wraith's hopes for a change in law enforcement's attitudes over telecommunications fraud in the post-RIPA environment:

> we'd like to think that we're not easily pushed over [by law enforcement]. We would like to be seen [as] having an important role and [...] as a [...] a partner with the police, rather than [them thinking]: "we can gain as much information as we'd like from you and you can't say no; you've got to just do it". It [...] doesn't work like that –it's a two-way thing [Fraud Control and Revenue Assurance Manager of a large UK wireless communications company, Int04:37-40].

> in the area I'm working in at the moment we're investigating fraud against BT. [A]nd, if we are seen as being adaptable and [...] law enforcement-friendly, when we go to them and say "will you help us to arrest these culprits?" they won't bring forward bureaucratic or procedural reasons –which they could. They could say "we have other priorities" –they've always got a murder running somewhere. They could say that they have priorities. They'll help us knowing that [...] we are professional and [...] police-friendly. So there's a bit of push and pull in it [BT Security Officer, Int07:145-151];

> Occasionally we want help from the police and [...], yes, it helps to have a good relationship. If they want some help from us, we give it on the idea that [...] when we want help from them we'll get it [CEO of large Internet service provider, Int08:279-282].

The question of whether there has been any direct or indirect connection between digital CI assistance by carriers and priority-designation to telecommunications fraud by law enforcement during CALEA negotiations was asked during all US interviews. Without exception replies were negative (see for instance Int16:202-205; Int17:192-197; Int19:771-788).

7.5.7. Challenging CALEA: Climbing the Hill.

While, in the UK, aggressive competition appears to have suppressed the effective collectivisation of the industry's voice in regards to IOCA and, later, RIPA, in the US, equally antagonistic market rivalries within industry appear to have been counteracted by a series of very sophisticated lobbying campaigns by the industry's well-paid

representatives. Once the industry realised that a CALEA-type legislation was favoured by a law enforcement-friendly Congress, its collective representatives concentrated their efforts on preventing law enforcement's access to technical standard decision-making processes (Int18:18-20, 20-24). By eventually achieving this, the telecommunications industry effectively denied US law enforcement and intelligence organisations the leading role in the technical design of digital CI. The effectiveness and thoroughness of the industry's lobbying efforts are recognised by both carrier and law enforcement participants in the negotiations on issues concerning CALEA:

> [we] organised a lot of [...] activity [...] up there [on Capitol Hill], because [...] the USTA, OPASTCO, the associations along with the [...] large [telecommunications] companies have a lot of people [...] who work at the [Capitol] Hill. This [...] is why some of the language [...] got [...] changed –because of a lot of the work. Because, when [CALEA] first came out [...] it was not very good at all. And then we went through the interviewing process, the compromise, etc [USTA CALEA lobbyist and point person, Int16:81-88; see also Int20:128-130];
>
> what CALEA represented was a compromise between the telecommunication industry, privacy advocates and law enforcement [CALEA Compliance Attorney, BellSouth USA, Int20:23-26];
>
> representatives like Don Bender and [...] others with [US]TIA and CTIA [(Cellular Telecommunications Industry Association)...] have a huge, powerful and influential presence with Congressional staffers, as well as with the Federal Communications Commission. I would say that we are mere blips at our relationship with government in that respect [...]. The industry has very well-paid talent[, people] that contribute to soft money, political action committees, not to mention their regular contributions to the political process [FBI Special Agent, CALEA Implementation Section, Int19:402-406];
>
> I don't think [that] we were really aware of the enormous lobbying power of the telecom[munication]s [industry]. I don't think we had [...] prepared for the challenge that we [...] faced. I don't think we could have [prepared], frankly [First Class Sergeant, Communications Officer, United States Special Forces, Int14:130-132].

Beyond their own ability to orchestrate sophisticated lobbying campaigns, what made the crucial qualitative difference between the legislative effects of US and UK CSPs on CALEA and RIPA respectively was the fact that the former were actually invited to a genuine round of negotiations by government. Hence, despite the legislators' national security-oriented preconceptions, the carriers were given "the opportunity, as an industry, to be involved" (Int17:125-127) in the debate. By 1998, the US

telecommunication industry's campaign had been effective enough to allow civil liberties observers to assert that "under CALEA, Congress made it clear that privacy interests and industry interests are paramount over law enforcement concerns" (Dempsey & Oram 1998). The underlying meaning of this statement is in considerable variance from the impressions of UK industry officials, who were involved in the RIPA debate:

> I think that [...] if there are suspicious motives [behind RIPA] being driven by, let's say, the Security Services or whatever, then there's not that much chance of getting them changed. They've got a lot more power and influence that any industry body has, so we're kind of [...] nibbling away at the edges [of the legislation] a little bit. If there is some fundamental, underlying [...] suspicious motive behind all of this, then [...] I'm afraid that there isn't much that we can do about it [Regulation Officer and law enforcement liaison of large UK ISP association, Int10:209-216].

7.5.8. Defending RIPA: Backdoor Lobbying.

Clearly, the above quote reveals a sense of being overpowered by political decision networks that are detached from mundane economic dilemmas, and operate on an exclusive level monopolised by national security priorities and concerns. In some cases, UK industry, as well as civil liberties-oriented interviewees, did air the belief that ministerial ears are intrinsically and freely lent to members of the law enforcement and intelligence services, who are often all too keen to remind elected officials of the non-negotiable qualities of democratic models of law and order:

> a party in opposition has all sorts of wild ideas about what it is going to do when it gets into government and [...] the policy appears to do a U-turn within days of getting into power. And you can't help but think that, in fact, it's not really [...] within days of them getting into power, but it's within days of them [...] having access to certain senior civil servants, who just say "I'm sorry, but this is the way it all works; we do need these powers for these very good reasons and, I'm sorry, we don't really care what your policy was when you were in opposition. You're in government now and you've got to change your tune. You've got to behave like government. You can't behave like the opposition any more". At which point lots of U-turns in policy get done at this kind of area [Regulation Officer and law enforcement liaison of large ISP association, Int10:229-231];

> from working in this area for a number of years, one certainly gets the impression that if you are a Minister and your security agencies come to you and say "well, look Minister, of course you can do what you like, but unless you give us these powers, in a couple of years you will have ghastly headlines about [...] gangsters running riot all over the country".

> And, if you're a Minister and you [...] don't really have any detailed knowledge of this area or the technologies or the criminology, you will ask a few questions but, basically, you have to trust what you're being told [Bowden 2000:241-248];
>
> [i]f you take an average politician to the MI5 or MI6 or Aldershot or Hereford or Cheltenham or any of these places [...],they sit in awe: "ah, there's all sorts of secrets in here; this is where James Bond lives and breathes". They're just in awe. They're absolutely in awe. They're like kids. They really are. It's pathetic, it really is. And they will just suck it all up. You know, who are we? We're just waiters...they don't care [CEO of large Internet service provider, Int08:170-174].

7.5.9. Defending CALEA: The Rhetoric of Emotion.

US Law enforcement agencies began pressuring for a CALEA-type solution during the late 1980s. They intensified their campaign in 1992 when it became apparent that the industry was not committed to a voluntary scheme of digital CI provision (Blair *et al.* 1995). There is little doubt that federal law enforcement made use of its direct access to the government in an attempt to gain a policy advantage over the industry:

> the [...] influence [...] of [federal law enforcement] agencies is [...] funnelled and directed through one or two voices in those agencies [...]. And they work quite gently with Congress. They cannot directly lobby Congress, [...] by law [...], they can only educate Congress. So there's some education that's going on there and [some] discussions [FBI Special Agent, CALEA Implementation Section, Int19:408-420];
>
> there were a lot of people in Congress that supported [CALEA] and the FBI was pushing it very hard [...]. I would suspect that the Department of Justice lobbied pretty heavily at the back room [Government Relations Director of a large national telecommunications association, Int18:17-18, 125-127; see also Int17:149-150];
>
> when you have as many FBI agents as they have and you send a bunch of them to Capitol Hill to do the lobbying...we often times found when we were lobbying that the FBI had been in just ahead of us with a bunch of agents and their Director [and] they'd been talking to influential members of Congress. This is why we made a lot of changes to CALEA early on and we couldn't get any later –because of the influence of the FBI [CALEA Compliance Attorney, BellSouth USA, Int20:170-175].

It is equally apparent that law enforcement's campaign was based less on technical and operational detail and to a much higher extent on emotional rhetoric focused on domestic terrorism targeted at US interests, and protecting children from paedophiles and other criminals. The example of a case where intercepted communications assisted the FBI in preventing the planned kidnapping and murder of a young child for the purpose of

making a 'snuff murder' film was constantly cited by proponents of enhanced digital CI capabilities for law enforcement at almost every given opportunity (Denning 1993; Barlow & Denning 1994). Other instances of carefully-constructed rhetoric included a 1994 public relations press conference, in which a law enforcement lobbyist, Detective Brian Kennedy of the Sacramento, CA, Sheriff's Department, remarked that what bothered him was that "there could be kids out there who need help badly, but thanks to this encryption, we'll never reach them" (Baker 1994; see also Anderson 1999; Freeh 1997b):

> we brought numerous instances, newspaper articles, clippings, sob stories, women who were carjacked and their phone was taken with them and we had to track the phone and get the content. So [....], we did a good bit of flag-waving [FBI Special Agent, CALEA Implementation Section, Int19:179-183].

There is evidence to suggest that, although this type of campaign was rather effective in recruiting elected representatives in favour of CALEA, it did not have the same impact on industry executives, who were primarily concerned about the legislation's economic impact on their businesses:

> I mean, every time we would go out to lobby what we would hear on [...] Capitol Hill was "you're going to take away the ability to go rescue people who are being kidnapped" or whatever. And [...] law enforcement uses that crime scenario very effectively [CALEA Compliance Attorney, BellSouth USA, Int20:167-170];
>
> I would say it had little effect on [the carriers]. And, after a while, we dropped that as a *modus operandi* because it just was water off the duck's back [FBI Special Agent, CALEA Implementation Section, Int19:181-183];
> politicians [were interested in] not appearing soft on crime and criminals, [whereas] the industry people were[:] "show me the money!" [...]. So we had to approach them in a different manner [First Class Sergeant, Communications Officer, United States Special Forces, Int14:139-141; see also Int17:150-152].

Ultimately, law enforcement's insistence on emotional rhetoric during lobbying campaigns might have helped them have CALEA approved by a Democratic administration, which was initially viewed as adversary to law enforcement's interests (Int19:374-375)[65], but it had little effect on the detail of the legislation, which was

[65] External observers, however, have remarked that the US President at that time, William J. Clinton, had been a supporter of CI since his days as Governor of the State of Arkansas (Willing 2000).

primarily controlled by the industry:

> our [campaigning] efforts were effective in that [...] a CALEA sort of plan was approved. But we [...] didn't get what we wanted [...]; we were not happy with most of the important provisions [...]. We wanted CALEA features implemented everywhere and [...] as soon as practically possible and that clearly didn't happen [First Class Sergeant, Communications Officer, United States Special Forces, Int14:452-455, 457];

> [CALEA's] first drafts were certainly more law enforcement-slanted than what came out of the [negotiations] [FBI Special Agent, CALEA Implementation Section, Int19-380-381].

7.5.10. Citizens' Participation: The Crucial Absence.

In an important sense, the introduction of CALEA and RIPA marked one of the rare instances in which the CI debate spilled over into the public limelight, with numerous articles on the subject appearing in the popular press. However, the negotiations that gave shape to the two pieces of legislation were largely, if not solely, monopolised by two complex and multifaceted sets of actors: law enforcement and the telecommunications industry. In the UK there were attempts by citizen-based civil liberties organisations to enter the upper echelons of the negotiations process. Although similar attempts in the past were rewarded with a modest degree of success, in terms of their impact on legislation related to electronic communications (Int01:142-145, HCTISC 1999a), RIPA was kept almost entirely away from the policy reach of such groups.

> in all these meetings and [...] regulatory initiatives no one is taking into account individual rights and liberties. The industry is concerned about their financial interests [and] law enforcement wants access to this and that [...]. So it is very difficult to establish a dialogue from the civil liberties perspective, because [we are] not IBM [(International Business Machines)] or even Demon Internet. Well, when you're Demon Internet or AOL [(America On Line)]they feel like they have to listen to you. But [...] who do we represent? [Akdeniz 2000:210-214, 259-266];

> the reality is that, [...] for as long as I have been involved in this [...], civil liberties representations are not formally recognised at all by the government. If you go back through the literature of press statements, the twists and turns of policies over the past three or four years, I don't think you will find one official acknowledgement of any civil liberties concern in any of this area –and one saw this through the debates on key escrow, as well [Bowden 2000:192-197].

In order to assume a position of relative influence, civil liberties groups attempted to approach the industry and introduce a civil liberties angle to the latter's rhetoric –a

formula that had been successfully carried out during an earlier debate on key escrow[66]. Indeed, it was this effort that led to the creation of Internet Users' Privacy Forum (IUPF), an industry/civil liberties scheme that remains unmatched in the US (see Cole 1999a; Cole 1999b). However, in approaching industry in this manner, civil liberties groups were somewhat forced to tone down their critical attitude against the RIPA[67], and eventually found themselves involved in the –not always wholesome– process of transforming their inherently political demands into consumer demands[68]. In addition, there is little evidence to suggest that the paramount industry actors paid any significant interest to the criticisms and propositions of the civil liberties community. In fact, the relationship between civil liberties and industry groups in regards to RIPA often appears adversarial. Few industry interviewees were prepared to condemn the civil liberties community on record, but, with the recorder turned off, many described the latter as "mosquitoes" –in the sense of annoying legislators while having little long-term effect– or "extremists":

> I guess for, say, the likes of Caspar Bowden and…and the people who are interested in the…Liberty and organisations like that, they…I mean…they have a different view. But [as far as we are concerned] the oversight process is there, in the […] last part of the [RIP] Bill […] and there is some […] recourse there. And [we] don't agree [with] all the people that are concerned about issues of privacy and personal security and […] going to an extreme [British Telecom Regulation Affairs Officer, Int11:320-326].

No detailed interviews were conducted in the US with civil liberties advocates, but a number of informative electronic messages were exchanged (Sehgal 2000; Cohn 2000; Courtney 2000). On the basis of the information provided in a number of these messages, it can be asserted that, although the impact of the civil liberties community on CALEA was not as powerful as ideally expected, civil liberties advocates were not

---

[66] "The industry didn't like their idea of key escrow and I can tell you that they [the government] wouldn't have listened to us, if it wasn't for the industry" (Akdeniz 2000:182-183; see also Bowden 2000:315-322).

[67] "You know, we don't necessarily say directly to the [industry's] face 'this is incompatible with the Human Rights Act and with the ECHR', because then you don't have a chance of negotiating with these people" (Akdeniz 2000:245-247).

[68] "[I]t is only industry lobbying that seems to be effective in changing government policy in this area […]. It is […] true that, if industry perceives that [a] large amount of civil liberties is concerned, then that tends to encourage the industry to be more forthright in their representations to government […] because, […] if the [industry] feels that they're […] being asked to operate a regime which [will] not be acceptable to […] customers in the market place, then that worries them on strictly commercial grounds" (Bowden:2000:205-211).

marginalised from the legislative debate to the extent that their UK colleagues were:

> [w]e were invited to participate in negotiations in late 1993, so we did have an opportunity to contribute to [CALEA] prior to its enactment [which was] in October 4, 1994 [Sehgal 2000];
>
> either through [members of] Congress or through the [telecommunications] industry, we were able to score a number of significant victories in [the] CALEA [debate], particularly with roving wiretaps and the [J-STD-025 or] J-Standard [Cohn 2000; see also Courtney 2000].

The relative impact of civil liberties on the legislation was also acknowledged by one law enforcement interviewee and even by industry participants in the debate:

> [the industry] took some hits from [...] the privacy groups, which w[ere] the Centre for Democracy and Technology, as well as EFF [(Electronic Frontier Foundation)...]. They too had input into the process and there was some give-and-take there [FBI Special Agent, CALEA Implementation Section, Int19:367-370];
>
> ah, they are very influential. Yes. Yes. The interesting thing about the [...] privacy sort of civil rights [issue], is that it's sort of a non-partisan issue and there you'll find [...] their members being from both the Democratic and Republican party that are very pro-privacy [...]. So, it doesn't necessarily cut off on party lines [Government Relations Director of a large national telecommunications association, Int18:115-121; see also Int17:133-137; Int16:131-135; Int20:368-370; Auble & Bender 2000].

Broadly-speaking, however, neither the UK nor the US digital CI debate was enriched by the adequate presence of grass roots, citizen-based organisations. There are reasons to believe that this unfortunate void was filled up by generalised assumptions about public attitudes held by the participants in the debate, which may or may not reflect reality and which may or may not have influenced the spirit of the legislation:

> I think that the vast majority of the public –and, after all, most of the customers of Internet service providers are the public– probably prefer society to be a safer place because of law enforcement's activities and therefore would say "well, of course you've got to go out and catch the criminals. I don't want my computer hacked, so please [act]. I don't want people sending me viruses, [so] please go out and catch these people and stop it happening to me" [...]. Therefore, I think, the public at large [...] is very pro-law enforcement. [I]f there was a referendum they'd bring back hanging, all right? And a lot of those libertarians forget this [Regulation Officer and law enforcement liaison of large ISP association, Int10:614-622];
>
> the public cannot be trusted to make a reasonable decision about [CI]. I

> think the public, when it comes to issues of cyber crime, will definitely err on the side of [...] law enforcement and say "yes, for heavens sake, can't they catch these people? Here, can I lend you my gun?" [ibid:627-630][69];

> you know, no, I don't [...] trust the general public and that's not just my [personal] opinion [...]. The general public usually –nine times out of ten– is incapable of handling the truth in these matters. Look at, for example, what happened with the death of Princess Diana in England. I mean, they just go mad. So, in my opinion, it makes absolute sense for some of these issues to remain confined to an executive [...] governmental level [First Class Sergeant, Communications Officer, United States Special Forces, Int15:631-637]

7.6.0. CI and Accountability.

It is perhaps this confinement of CI-related information to executive governmental levels that has historically sparked a number of popular and academic debates about the degree of accountability, or lack thereof, that characterises state-sponsored CI practices and practitioners (Fitzgerald & Leopold 1987; Theoharis 1971). The fact that there is little documented information about illegal CI by law enforcement agencies in the US and the UK has not prevented civil rights watchdogs from being suspicious:

> as to what's been done in the past, [...] most of what one hears [...] is anecdotes. But there certainly are plenty of anecdotes [...] right up to the present day, about informal approaches being made to telecommunications companies and access being granted [...] on a sort of first-name-term 'matey' relationship basis, both to the communications data and to content without a warranted procedure being in place [Bowden 2000:467-472];

> [i]f you build an infrastructure that encourages wiretapping, it will be abused. The only question is: "how many years or decades will it take to find out it's been abused"? [John Gilmore, EFF Co-Founder, ctd in Poulsen 1999].

In the UK, the closest government sources come to admitting instances of illegal wiretapping is by reporting for the public record a number of instances where CI operations have gone wrong. Such instances are published in the Interception Commissioner's annual report to Parliament. The following characteristic quote is from

[69] Reflective of this attitude is a comment made by former UK Minister of State Jack Straw in Parliament: "I also explain to constituents at my surgeries that, given the weight of the threat from international crime and terrorism, the prospect is remote that we would devote resources to intercepting their telephone calls. However, I then provide no reassurance when I say that I cannot tell them whether their telephone is the subject of intercept because otherwise others who might be the subject of intercept could come along on fishing expeditions. It is logically a difficult position to explain to individuals, and it is difficult for people to understand that" (House of Commons 2000).

the latest such report:

> [in one] case the Security Service applied for a revalidation of a warrant, but the submission listed an incorrect operator. This initial error was not identified by the Home Office and the warrant was renewed including the incorrect operator. This renewal was therefore invalid. This error only came to light when an approved request to modify the warrant to delete one number and add another was submitted to the original operator. The error was compounded by the fact, confirmed by subsequent investigation, that given the particular circumstances of this operation, the intercept had not been suspended when it should have been. This increased the period of unlawful interception. All product from the total period subject to the error has been destroyed. The error reflects badly on all parties concerned, the Security Service, the Home Office and the operators involved [Command 4778:§45].

Such incidents –which are not few– are usually attributed to erroneous judgements and logistical shortcomings. But UK interviewees painted a rather different picture, namely one where illegal CI and data acquisition by law enforcement are often the outcome of calculated intent, rather than human error:

> [t]hings do go wrong. In the past, the typical things that have gone wrong have been like, sort of, a police officer who suspects his neighbour of having an affair with his wife and [...] wanted to find out if she'd phoned the mobile or something like that [BT Security Officer, Int07:107-109; see also Int08:298-305];

> I wouldn't [...] say that there isn't any [illegal CI] going on, because I would be lying. It does happen, though I know it's rare nowadays. It depends on the arrangements with local constabularies. When I started working [for] BT, I mean, there would be times when officers would [call] the technicians [...] and request information, rather than going through [the] local branch managers. I mean, because they would eventually get to know each other and so [...] that's what would happen [former British Telecom external maintenance engineer, Engineering Division, Int03:401-408; see also Parr 1999; HCTISC 1999b].

Another phenomenon, which usually occurs with the larger, more established telecommunications companies, is that they will often make considerable effort to honour law enforcement requests, despite the latter's lack of proper authorisation, and while remaining within the 'spirit' of the law:

> I'll give you an example: somebody says to [us]: "we want an ex-directory number" and we don't want to give them that ex-directory number unless we have to. So [...], then we say: "why do you want it?". And they say: "we want to telephone this person". Then we say: "fine, we'll set the call up for you and you can speak to them, but we won't give you the number". Then we avoid having to do the rigmarole for giving them permission for an ex-directory number. So we [...] don't

> have to give them the number, but they get what they want. And this is [...] I mean, [such] examples [occur] very often, I would imagine [...] certainly on my team, in the past, when we've handled it [...]. We would say to them "you can't have that but you can have this and it solves your problem". And so [...] we wouldn't refuse. I don't think we would ever refuse [...] a request arbitrarily [British Telecom Security Officer, Int07:127-138][70].

One former Special Branch officer explained that most unauthorised law enforcement-sponsored CI concerns the acquisition of communications data, rather than content, because it is easier to obtain, and can be facilitated by the carrier without the requirement of much logistical support. This practice, which is known in industry and law enforcement circles as a 'fishing operation', is quite straightforward and can involve a large number of telephone subscribers:

> [i]n the past it [...] has not been unknown for law enforcement agencies to 'fish'. [S]ay they put in a suspect and on the suspect there are six telephone numbers and for some reason they relate this to the crime in hand. So, they ask for the subscriber details on the six telephone numbers and they are provided.
>
> **Q:** OK, so that's a fishing operation.
>
> **A:** No, it's not. The fishing operation hasn't even started yet. They get the six numbers and then come and say "we want the billing record for the last 3 months for these six people. That's the fishing operation. And they should then get the billing records and they go from the billing records to see who their six people have called. And then you say "right, let's analyse those; and let's get the billing records of those 500 people"; and you can see how you can build that up. Now, with the modern analytical tools you can put all that information in and you can get a picture out. Right. But that's a fishing expedition –because, at the end of the day, whilst it would be quite genuine for the first six [people], no way is it genuine for the six billing records, over whatever period, for those six [people]. And you then start to move away from what is immediately involved [Former Special Forces Officer, Int12:409-425].

However, the interviewee –who has had experience in working for both the Secret Services and, later, telecommunications carriers– went on to assert that this practice has been gradually fading out ever since BT's privatisation and the introduction of a number

[70] On the whole, downright refusals of law enforcement CI requests are very rare on both sides of the Atlantic (for the UK see Int04:154; 156-158; Int06:96-98; Int07:117-118; Int08:264-265; Int09:260-261; Int10:289-290; Int11:474-477). According to one FBI interviewee, there has been only one case in living memory when a carrier refused to honour a request (Int19:573-592). But other FBI sources have revealed that "there have been anecdotal reports of instances where carriers have refused to provide assistance to Law Enforcement even after being presented with a facially valid court order in circumstances where carrier personnel 'did not recognise' a particular judge's signature or where the description of the carrier service to be included in the intercept did not precisely match the carrier's

of legislative safeguards:

> I know of instances where, two years ago, 'A' would ring 'B' and say "who is on this telephone number?" and B would say "no problem Mr Smith". [T]here was no accountability. No one in the past has had to account for [...] anything. You know, I mean, [...] we've only got to go back, I suppose, ten [or] fifteen years, that if a policeman said to you "I want to know about ABC", because he was a policeman, you'd tell him. I mean, you know, he was the policeman, it was his job, he was investigating so you'd tell him [...]. In terms of the industry, [there have been] arrangements with law enforcement, which have not necessarily been as tight as they should have been. But that now is a thing of the past. I mean, now no one gets any information, personal details of any customer or any subscriber, unless there is a clear order to put trail on where that information is going and why it is required. I mean [...], I have seen [it in] recent cases; I mean, that's a sea of change in the last few years, brought about mainly by [the] DPA [(Data Protection Act) 1998] and the requirements for DPA [and] re-enforced by the changes in the Telecom[muniation]s Act, in [the] Freedom of Information [Act], in [the] European [Convention on] Human Rights, [which] has been proposed in the UK legislation, in terms of human rights [...]. In the past, the fact that the documentation didn't follow through was neither here nor there. Now it has to. And if it's not, then within 24 hours the company is back to that Police Force in question and wants to know why [...]. If they rung 'B' today, 'B' would say "DPA form" –end of story. And it [...ha]s happened in recent past almost on a daily basis [and] it's getting to the point now where 'A' wouldn't even ring 'B' unless there was a DPA form –end of story. So there has been a much tighter control in that level of information –that lower level of information [...]. I wouldn't hand-on-heart say "it would never happen". Because, you know, at the end of the day, police are police, they're human beings and [...] will try [...] it on sometimes –no doubt. But they will get short shrift to where before they got almost [...] blind obedience, because [...], at the end of the day, they were the good guys, they were asking and were given it [ibid:327-395, 430-435][71].

There are strong indications, however, that non-warranted law enforcement-sponsored CI requests are occurring increasingly in the ISP industry, where both law enforcement and carriers are unsure as to the legal requirements that have to be present before CI can be facilitated (HCTISC 1999a; Int01:307-309; Int05:454-457). Consequently both sides usually choose to opt out of the warranty process completely:

> **Q:** [Y]ou don't have to answer this question, but, according to your knowledge, have communications service providers, ISPs in our case,

---

brand name for that service" (Morris 1998; see also Dempsey & Oram 1998). The last such incident before the enactment of CALEA occurred in 1968 (Boucher & Edwards 1994).

[71] In a 2000 presentation before a large group of law enforcement liaison officers of UK wireless and wireline carriers, the UK telecommunication's industry's designated Single Point of Contact under RIPA, Jack Wraith, said "[w]e've all at some time or another experienced a policeman ringing us up at some ridiculous hour saying: "this is urgent, this has got to be done" only to find at some later date that was not the case. Hopefully, fishing expeditions are a thing of the past –and we've all had them" (Wraith 2000).

always been served with warrants prior to assisting law enforcement with [...] interception of communications?

A: I haven't had a single warrant. In all the occasions the cops were completely flatfooted. They had no [...] idea what they were doing. What they were looking from us was whatever they could get [...]. They came out here and they said: "we'll get you a warrant" and...whatever. They said: "the reason we haven't brought one is we're not quite sure what it is we're applying for". They said: "can you show us what you've got and what you can do?" [CEO of a large UK ISP, Int08:203-211, 219-222][72];

[a]t present, the police regularly make us aware of a serious crime, which they cannot investigate without us providing contact information for one of our customers. They know the Internet identity of the person they wish to investigate but only we, as their ISP, can link this to a real world identity. We are able to supply this personal information [...]. We believe that this arrangement (famously described by Peter Sommer as "cosy"), which does, of course, allow the police investigations to proceed when they would otherwise be stymied, will break down in the face of a specific commitment to our customers that their personal details are confidential. In the relatively near future ISPs are likely to insist that the police always have a warrant before data can be made available to them [Hall *et al.* 1996][73].

In the US, instances of unauthorised state-sponsored CI are equally common, though industry and government sources are usually unwilling to discuss them. In 1998, for example, a Los Angeles Deputy Public Defender discovered that officers in the Los Angeles Police Department had concealed the role that unauthorised CI operations had played in as many as 425 prosecution cases since 1993. Content acquired through the illegal operations had been used to prosecute and convict defendants, but it was never disclosed to the court that they were obtained through CI methods. In the same case it was revealed that police officers had manipulated public CI statistics by using a single court order to obtain multiple taps on many individuals. It was reported that

> [o]ne order, facilitated with the help of a cellular telephone carrier, lasted two years and involved the wiretapping of 250 phones, but was reported to state and federal authorities as a single surveillance [Poulsen 1999].

One interviewer, a US Special Forces Communications Officer with specialist technical

---

[72] For similar instances in the US see (Feldman 2000): "[t]he smaller ISPs are generally the worst in protecting your confidentiality. They 'roll over' easily. I've called and they've told me the guy's real name over the phone without a subpoena or anything".

[73] ISP representatives have also complained to Parliament that on numerous occasions police require them to "check their records just to see if a suspected criminal might possibly have an e-mail address" (Delio 2001). "Rachel Basger, regulatory manager of World Online, said that she had been asked [by law enforcement] to provide a list of users who had a specific zip code shared by someone who was under investigation, just in case the suspect had an account with World Online. 'Perhaps I got the

training in CI operations, described how law enforcement are able to evade effective public oversight in CI investigations:

> say you're [...] Police Detective Doe –right?– investigating a car thief, right? And you [...] apply for an [...] intercept [warrant] and you get it, so you start intercepting the car thief's [telephone] calls, right? Well, [...] then you find out that the car thief has been talking to a drug pusher on his phone. But you can't move in to arrest the drug pusher, [be]cause you don't have a probable cause. So, what do you do? You [...] hand over your [intercepted data] to your fellow Police Detective Roger, who then goes ahead and uses it to gather separate evidence and then arrest the pusher –see? So [...] that's what they call a "hand-off technique" [First Class Sergeant, Communications Officer, United States Special Forces, Int15:189-198].

A number of interviewees also disclosed that, historically, a considerable percentage of law enforcement-sponsored CI operations that occur in small-town and rural areas of the US has been unauthorised, and it has usually been facilitated through the informal relationships formed between law enforcement and carriers in small-town settings:

> you [can have the] sheriff coming in [to the local carrier's offices] saying "hey, so and so is squabbling with his wife, can you [...] listen in?" –you know. But [...] small types of things like that aren't Title IIIs and it's [...] been done for years in [...] small [telecommunications] companies. They all understand. It's a right. They're good [...] citizens and it's their [...] obligation to do so [Technical Director of a national telecommunications association representing more than 500 small-sized and rural member companies, Int17:55-62];

> [b]efore [the AT&T breakup] we just called them [to request assistance]. When I called over to their centre and said who I was, they even knew our operators. They said "oh, yeah, what's the trouble, [his first name]?". We had a policy that anytime we had a new employee or any time they had a new employee at their phone centre we sent our people over there to [...] meet the people, to see the equipment, to see what they were doing. When they had a new employee they'd come over here and [...] and we did the same thing. They would come over, we would send our person and they would meet the new [...] employees [...]. And then those people would send their people back. So we tried to –as much as we could– not to let it go more than 90 days before a new employee on either side coming and meeting one another. So that when ['A'] calls ['B'], he knows that ['B'] is a little fat, short, bald-headed guy and he knows where he's at, he knows what his equipment is and a little bit of his personality, [be]cause he sat and talked to him some [Technical Unit Chief, Emergency Communications Unit (organisation withheld for privacy reasons), Int13:153-164].

7.7.0. Summary.

---

short straw and pulled the only really stupid request. But from what I hear, I worry that it was not an

Digital CI legislation has been a contentious issue, partly because of the dependence that UK and US law enforcement maintains on the practice as an investigative technique. This crucial dependence is recognised by the carriers, who are either compelled by legislation or by corporate citizenship principles to assist law enforcement.

The industry is generally split on whether RIPA and CALEA are technically achievable, though it appears that, even if they are, the future evolution of digital telecommunications networks will render large segments of the legislation inapplicable. Nevertheless, RIPA and CALEA were partially introduced to allow law enforcement to bypass its lack of technological knowledge by rendering industry professionals responsible for carrying out sophisticated digital CI operations. This would mean that in the fully implemented RIPA and CALEA environments, industry engineers would be conducting 100 per cent of CI investigations. This could have the effect of making carriers more engaged in questioning the legal justifications of CI operations. It would also place carriers in the centre of the battle for power between groups aiming to increase their CI capabilities and groups aiming to augment their communications security. This worries both the carriers and law enforcement, who will effectively lose control over the micro-mechanics of CI under RIPA and CALEA. The two groups, however, are gradually being drawn closer by the legislation's operating model.

Another partial reason why RIPA and CALEA have been introduced is to tackle the large number of actors that are now part of the mushrooming telecommunications sectors in the US and the UK. This has been a direct outcome of the sector's deregulation, which took place in the 1980s. It produced both financial and cultural shifts, which have drawn industry further away from its once intimate relationship with law enforcement.

The negotiations between law enforcement and industry over RIPA and CALEA were largely held in secret, and few details are known about them. Neither of the two sides were unified in their interests, and this had a negative impact on the industry's ability to shape the legislation, especially in the UK. One of the few negotiating cards that the UK industry was able to use was its offer to be cooperative under RIPA in exchange for more attention paid to telecommunications fraud by law enforcement. The US industry had higher success in negotiations over CALEA, and so did the US civil liberties lobby, which worked in cooperation with the industry. In contrast, the UK civil liberties lobby was excluded from negotiations over RIPA.

The implications of the findings presented in this chapter will now be discussed in the following chapter.

---

isolated incident', Basger said" (ibid.).

Part IV DISCUSSION AND CONCLUSIONS

Chapter Eight

Future Trajectories of Interception

8.0.0. Introduction.

This chapter discusses some of the findings outlined in chapter seven, in relation to the wider literature on the subject. Following a comparison between the UK and the US CI debate, there will be a discussion of the impact of market deregulation on state-sponsored surveillance structures on both sides of the Atlantic. The technical integration of CI mandates into the telecommunications network infrastructure under RIPA and CALEA will also be analysed in light of legal, political and cultural developments shaping the context of state-sponsored surveillance. Finally, there will be a consideration of the importance of the intelligence factor in shaping the future of domestic CI practices in the 21st century.

8.1.0. Comparing Transatlantic Case Studies.

Significant similarities were established in the course of this research between UK and US debates on digital CI. Admittedly, many of these similarities are due to the common technical features that mark the two nations' digital telecommunications networks, which gave rise to roughly similar legislative measures to restore state-sponsored CI capabilities. The broadly similar market framework that characterises the deregulated UK and US telecommunications industry is also responsible for some of the similarities found between the two nations' CI policy. Thus, for instance, both CALEA and RIPA

appear to be transferring control over CI from governmental agencies to private carriers (section 7.3.0). In addition, both UK and US law enforcement agencies appear rather apprehensive over this imminent loss of control over the micro-mechanics of CI (section 7.3.2) and there is a sense of alarm about an already detectable tendency by telecommunications carriers to evaluate the legal justification of CI requests (section 7.3.1; see also section 8.2.1 below).

Also traceable are similarities in the nature of the impact of market deregulation on the UK and US telecommunications industry in relation to the digital CI debate. Thus, both industries appear segregated between older and younger carriers; the former are characterised by a sense of reassurance about their historical arrangements in facilitating state-sponsored CI, while the latter have often ambiguous feelings about assisting law enforcement and often refuse to honour CI requests in the absence of sufficient documentation (section 7.5.4). Furthermore, the increasing competitiveness of the UK and US markets appears to have filtered law enforcement concerns out of the day-to-day running of telecommunications. This new environment has shaped a different generation of private carriers who are less willing than their state-protected predecessors to place law enforcement and security concerns over their immediate and long-term financial goals (section 7.5.0).

Equally significant are differences that appear to mark the CI developments in the two nations. During interviews, for instance, UK carriers appeared more willing than their US counterparts to distinguish significant political implications in the abuse of CI by government authorities (section 7.1.0). They were also not very optimistic about the technical prospects of implementing comprehensive CI capabilities in the digital environment. On the contrary, having been subjected to CALEA scenarios for almost a decade, US carriers appeared much more prepared to overcome or bypass some of the more complex technological barriers to state-sponsored CI –providing, however, that substantial financial resources from public funds became available (section 7.2.1).

Although, similarly to the UK scene, the telecommunications industry lobby in the US is primarily fragmented and antagonistic, US carriers were able to have a stronger say in shaping CI legislation (sections 7.5.4; 7.5.5; 7.5.7), probably because they managed to achieve a high degree of unity against the US government. Furthermore, it also appears that the US administration was much more willing to consider industry and civil liberty

concerns over CALEA seriously (section 7.5.7). It was probably the absence of a will for a genuine dialogue on behalf of the UK government which forced the UK industry lobby to resort to a form of bargaining in negotiations over RIPA, by requesting increased assistance from law enforcement in combating telecommunications fraud, in return for adopting a co-operative stance over the proposed legislation (section 7.56).

8.2.0. CI in a Deregulated Market Environment.

The scant literature on domestic CI indicates that, ever since the beginning of telephony in the US and the UK, the lines of demarcation between the telecommunications security and law enforcement communities have traditionally been rather faint (section 5.6.0). Indeed, in numerous instances, such as during the two World Wars or at the peak of the Cold War, these lines were almost totally obliterated, allowing for the establishment and maintenance of a set of aggressive CI policies in accordance with the mandates of national security. Research conducted in the context of the present thesis appears to confirm this intimate institutional interface and points to the endurance of this phenomenon until fairly recent times (sections 7.40; 7.6.0). In the UK there is also evidence to suggest that, in some instances, law enforcement agencies have used what they perceive as absence of regulation in regards to ISP-facilitated CI[1] to conduct unwarranted surveillance of Internet data and content.

But the findings of this research also suggest that this tradition came to an abrupt halt with the telecommunications deregulation of the 1980s and 1990s, which resulted in a dramatic severance in relations between the industry and law enforcement agencies in both the US and the UK. Indeed, the extent of the deterioration in relations between these two once closely linked sectors can hardly be overstated. The decision to end the AT&T and BT state-sheltered monopolies literally pulled the rug under the feet of law enforcement and security agencies by greatly increasing the numbers of actors involved in commercial telecommunications. The UK telecommunications market was once synonymous with BT. Today, however, it is estimated that the industry consists of no less than 200 PTOs and several hundred ISPs. In the US, where the government's

[1] A perception which, according to NCIS, is erroneous: Mar Castel, a policy expert at the NCIS Special Projects Branch has testified that the IOCA 1985 would be adequate to warrant cases of Internet-based interception: "[i]f the transaction is happening over a public telecommunication network then [the IOCA 1985] does [cover ISP-facilitated CI]. But when the data is at rest with the Internet service provider then the Interception of Communications does not cover it; but the Pace Production Order, which is issued by a High Court Judge, would cover it" [HCTISC 1999a].

interception agencies were used to dealing with less than a dozen carriers prior to deregulation, there are today in operation approximately 37,000 carriers of all descriptions, more than half of which did not exist in 1994 (see section 7.4.1). The once exclusive gentlemen's club of CI (Int11:20-26) has disintegrated by virtue of the phenomenal rise in the sheer numbers of its candidate members. These crucial developments, which are hardly recent, have not been traced by the scant relevant literature, which has tended to concentrate on official documents (Diffie & Landau 1998:183ff; Sutter 2001), thus missing out on a number of tacit trends occurring on the day-to-day level of CI practice.

Not only is the relationship between the intercepting agencies and the new, private sector CSPs largely unstructured and unformed (see section 7.4.3), but the financial and logistical impact of the imposition of RIPA and CALEA over the larger, more established carriers, has had a diminishing effect on their relationship with government agencies, especially in the US:

> as CALEA implementators –whatever that is– we're the last person [the carriers] want to see. When you say CALEA it is like dropping acid in their eyes [.... W]hen it comes to CALEA [...] our relationship with the carriers and those who are dealing with all of that has been diminished [and is] adversarial in some cases. CALEA [ha]s really been a detriment to the relations that we previously enjoyed –at least with that small family of carriers– and [...] right now I don't see any recovery or normalisation of a good and strong working relationship between the carriers and law enforcement. I haven't [...] witnessed it. If anything, it's getting more fractionalised –worse [...]. We need [the carriers], they don't need us. It's really odd, because [...] we're implementing this law and we're creating enemies [...] of people that we can't afford to [have as] our enemies. It's really tense [FBI Special Agent, CALEA Implementation Section, Int19:451-453, 809-816, 846-848].

Consequently, there is little doubt among industry experts on both sides of the Atlantic that the immediate and long-term future of digital CI legislation will be marred by consecutive legal challenges and court battles, which will further strain relations between industry and law enforcement:

> the RIP Bill seems to proliferate the thinking that "let's get it into a Bill and let the courts decide in the long run". We suspect –certainly the general feeling on the streets is– that the RIP Bill will get through, but a lot of the issues therein will not be cleared until someone has been taken to court and the highest court in the land has made a case [...]. Now, if [the industry] were to take that line, then the system would break down overnight because there is no way that the justice system could go through that process every time one wanted the name of a [...] telephone

> [...] subscriber or what have you [TUFF fraud and law enforcement liaison officer, Int12:108-113, 257-260];
>
> most of ISPA, they're ISPs that are big enough, they don't need to bother about the government. They're taking the attitude that "well, OK guys, you roll it out and we'll test it in court". The RIP[A] is a big sledgehammer: "you will co-operate". Or will we? It's not very well thought out. Not very well thought out at all [CEO of large UK Internet Service Provider, Int08:88-92, 291-292; see also Int05:225-229; Int10:160-164; Int11:163-168; Parr 1999; Dempsey 1995];
>
> as far as CALEA itself, I think we're just seeing [...] an evolving type of law that's going to have challenges after challenges and implementation schedules changed as standards change [Technical Director of a large US telecommunications association, Int17:215-217; see also Int13:216-221; Int19:389-393];
>
> a year ago, when times were good, everybody leaned towards the view that it was better to not pick a fight with the FBI. Now it's less clear that people have the funds to spend on development or to purchase this [CALEA] stuff, so there could be a serious conflict over this [Stewart Baker, former NSA General Counsel, ctd in Brown 2001].

On a broader note, it is apparent that the restructuring of capitalist relations in the UK and US telecommunications industry –as symbolised by the drive toward a less regulated and more competitive market environment– has delivered a serious assault on the ability of centralised governments to police the pattern and content of their citizens' communications. In this sense, and if CI is to be seen as part of the overall surveillance capacity of contemporary state apparatuses, it would seem inappropriate to equate the evolution of capitalist systems with an inherent increase in the level of government surveillance[2]. As this study shows, the often chaotic complexity introduced to rigid state-sheltered systems of communication by economic deregulation can result in the disablement of surveillance structures that have not been designed with deregulation in mind. This disablement does not have to be permanent. For instance, it may not be long before new CSPs are introduced to the principles of US and UK national security mandates; yet much more time, resources and political skill will be required before CI legislation can reflect the increasingly global structure of the deregulated telecommunications markets (see section 7.4.2).

[2] As is done, for example, in Ackroyd *et al.* 1980 or –to a lesser, though still considerable, extent– in Gandy 1993.

8.2.1. Industry's Enhanced Role in CI.

On the contrary, it would appear entirely appropriate to suggest that, in a deregulated environment, where the legislative and political authority of government intervention is structurally minimised, the surveillance capabilities offered by enhanced digital technologies are not thwarted as such, but rather heavily controlled by corporate institutions to the detriment of state agencies. This assertion would be in agreement not only with the overall spirit of capitalist deregulation, which aims to marginalise the role of government in the affairs of civil society (Hills 1986:25), but also with the findings of this study in regards to the enhanced role of CSPs in the implementation and oversight of CI operations under RIPA and CALEA.

As explained earlier, in sections 6.3.1 and 7.3.0, according to interception models favoured by both RIPA and CALEA, for the first time in the history of CI, 100 per cent of standard wiretapping operations will have to be performed by the carriers, rather than by law enforcement. Clearly, this shift in the paradigm of state-sponsored CI signifies a loss of control by government agencies of the technical process of CI.

In addition, it would be unrealistic to expect that carriers can assume complete technical responsibility over state-sponsored CI without eventually being drawn into a more engaging legalistic role in CI operations. Indeed, as shown in section 7.3.1, there is already evidence to suggest that UK and US carriers are beginning, or intend to begin, to query the justification of state-sponsored CI requests. If this trend continues, then, inevitably, the carriers' upgraded role in safeguarding their users' privacy –which they see as a revenue-generating feature– will attract considerable pressure from groups or institutions aiming to either increase their CI capabilities or augment the security of their communications (section 7.3.2). In an important sense, therefore, RIPA and CALEA appear to be recognising the enhanced control of the private sector over the privacy –or lack thereof– of citizens in the information society.

8.2.2. Deregulation an Anathema to CI.

In the UK, this shift of CI practices from state to industry is partially due to British law enforcement's lack of technical knowledge about the specifics of digital communications systems. Indeed, British industry representatives who maintain daily contact with law enforcement and intelligence officials have formed an impression of the latter's

technological expertise that varies immensely from popular –and often academic[3]– myths of highly sophisticated government techno-agents making use of super-advanced interception gadgetry. In reality, British law enforcement officials are considerably under-trained and lack basic knowledge about the fundamental features and capabilities of digital networks, including the Internet (section 7.2.2).

Nevertheless, the aforementioned shift in CI is also partially due to the particular design features –rather than the overall nature– of digital technology itself, which tend to largely diminish the potential of tampering with the networks at the local loop, or even at the cross connect box (section 6.2.1). In other words, there is nothing intrinsic in digital networks that renders them more resistant to interception than, say, analogue networks. Rather it was the absence of law enforcement and intelligence interests from technical decisions on digitisation that resulted in the marginalisation of such interests from the very design of digital telecommunications systems (section 7.2.1).

This latter point is potentially more significant than it may initially appear: for law enforcement, CI is not simply another investigative tool; as explained in section 7.1.0, there is a long historical tendency within the law enforcement establishment in the UK and the US to regard CI as a fundamental pillar of investigative competence. Yet, in spite of that, UK and US law enforcement and intelligence agencies had limited and ineffective input in early debates on telecommunications digitisation or even in later debates concerning the standardisation of these technologies. When asked what was the logic –if any– behind this absence, law enforcement officials replied that it was simply none of their business:

> [It all began w]hen they denationalised…when BT lost their monopoly, basically. And…
>
> **Q:** Didn't law enforcement people sort of forecast that? Or didn't they realise it was going to happen?
>
> **A:** I mean…no. I mean…they are not part of that discussion […]. Denationalisation and de-monopolisation, or whatever you'd like to call it, was created in order to provide market forces and the best commercial aspects for UK liberties. Law enforcement doesn't come into that […. Take, for instance,] the introduction of pre-pay [mobile phone systems]. Law enforcement was very, very much against [them] –had it been given an opportunity. It would have been virtually against by the law enforcement [community]. But, no way, they are not consulted, you see, they are not part of that consultation process […. So,] whilst law

[3] See for instance Manwaring-White 1983.

> enforcement don't like [denationalisation], I think they would agree they're not part of that discussion. It's outside their limit [Former UK Special Branch Officer, Int12:464-467, 469-472, 486-489, 501-502].

> I realise that from a commercial perspective [...] there [wa]s a reason for the break up of the [AT&T] monopoly. But from an [...] overall quality control and an overall tracking of telephone service it has been very bad and it's getting worse [.... W]hen they broke up AT&T, the FCC or the Federal Government [...] didn't look at the whole picture. Deregulation on one hand is good for the consumer [...], but on the other hand, for public safety and for the consumer not knowing it was very bad. [T]hat part of it was never looked at. And if you talk to these people they'll say "oh, yeah, oh gosh we shouldn't have done that". But nobody investigated this side of it. Nobody asked. The people that were putting the pressure on from the commercial side were putting so much pressure on that the half-paid attorneys and what have you were pushed, pushed, pushed. They didn't tell –they didn't want that to come out because that would influence the court's decision on "do we need to do this or is it really that good for the market?". It's been bad for us. At this point in time we just have to fix what we've got [Technical Unit Chief, Emergency Communications Unit, Int13:49-52, 84-85, 97-106].

In the US, even the FBI itself has recognised the subordination of its perceived security interests to the interests of a deregulated and commercially-driven national economy within the global capitalist environment:

> [t]he United States has traded the comfort of uniformity and predictability in its communication system for creative innovation and vigorous competition [...]. The goal of the [CALEA] legislation [...] is not to reverse those industry trends. Indeed, it is national policy to promote competition in the telecommunications industry and to support the development and widespread availability of advanced technologies, features and services [Blair *et al.* 1995; Boucher & Edwards 1994].

There are strong indications to suggest, however, that this relinquishment of national security mandates in favour of capitalist restructuring did not come about smoothly. British academic analyses of telecommunications deregulation contain little evidence of national security concerns having been fed into this primarily economic debate[4]; but in the US there are clear indications that at least some segments of the nation's security establishment wasted little time in strongly opposing the Reagan administration's intentions to break up AT&T (Judge 1985:passim). As early as February 1981, only a

[4] Though actors did express concern about the lack of "expressed vision" and of "long-term objectives" in the British government's deregulatory drive (Veljanovski 1991:20ff). The fact that there is little evidence in the literature about the telecommunications deregulation debate being marked by national security concerns should not necessarily be taken to mean that such concerns were not aired. Rather, it is likely that they were communicated away from the public domain by members of the UK security establishment or even that academic works on the subject have failed to notice this element in the debate.

few days after moving into the Pentagon, US Secretary of Defence Caspar Weinberger communicated in a memorandum to US Attorney General French Smith his Department's vehement objections to the antitrust lawsuit against the company:

> [t]he purpose of this letter is to express the deep concern which the Department of Defence feels over the reports of the proposed settlement of the government's old antitrust suit against the American Telephone and Telegraph Company [...]. Our concern is based upon the fact that a great deal of the current capability for communications command and control of our strategic weapons depends upon the continued existence of the only communications network in the United States capable of providing the services required [...]. The Department of Defence recommends very strongly that the Department of Justice not require or accept any divestiture that would have the effect of interfering with, or disrupting, any part of the existing communications facilities or network of the American Telephone and Telegraph Company that are essential to defence command and control [Caspar Weinberger ctd in Carter 1989:224; see also Tunstall 1986:104][5].

The Department's strong stance against the AT&T divestiture was also communicated by the then US Deputy Secretary of Defence, Frank C. Carlucci, in a letter addressed to US Assistant Attorney General William Baxter[6]. In it, Baxter was urged to consider the "severe problems [that will] confront the Department of Defence if this network is broken up" (Frank C. Carlucci ctd in Carter 1989:225). Carlucci helped compile an additional 1981 report by the US Defence Communications Agency, which effectively became declassified when it was introduced to the US government's antitrust trial by AT&T's legal team. The report stated that the DoD

> can unequivocally state that divestiture [...] would cause substantial harm to national defence and security and emergency preparedness telecommunications [because it] would substantially reduce or eliminate entirely the incentives [...] to engage in that prior joint [–among different service providers as well as between providers and government–] planning and preparation [necessary] to conduct centralised network management. The Defence Department totally disagrees that divestiture would have no adverse effect on the nation's ability to rely upon the

[5] Weinberger reiterated his Department's concerns a month later in testimony before the US Senate Armed Services Committee, in which he stated that "[t]he American Telephone and Telegraph network is the most important communication net we have to service our strategic systems in this country. Because of the discussions I have had concerning the effect of the Department of Justice suit that would break up part of that network, I have written to the Attorney General and urged very strongly that the suit be dismissed, recognising all of the problems that might cause and because of the fact it seems to me essential that we keep together this one communications network we now have, and have to rely on" (Caspar Weinberger ctd in Carter 1989:224).

[6] Baxter was also Head of the DoJ's Antitrust Division.

> nationwide telecommunications network. Instead, we believe that it would have *a serious short-term effect and a lethal long-term effect*, since effective network planning would eventually become virtually non-existent (ctd in Bolling 1983:53-54, emphasis added).

Yet, despite the strong lobbying by US Pentagon officials, Congress and the FCC remained unmoved[7] (Carter 1989:224) and, eventually, the Reagan administration decided to implement the break up of AT&T in direct confrontation with the nation's security community. Evidently, deregulating the US telecommunications sector was of immense symbolic significance for the Reagan administration's broader liberalisation programme (Hills 1986:24ff). and its completion was considered to be more politically meaningful than the protection of equally important, yet less prominent and less voter-worthy, national security mandates.

This incident would appear to lead us to the assertion that, when it comes to surveillance and telecommunications policing, inner policy coherence between different sectors of the contemporary state apparatus should not be presumed. In fact, some writers point toward policy inconsistencies within the DoD itself, whose officials were against national telecommunications regulation, which they saw as adversary to C3I goals, while at the same time favouring global liberalisation of telecommunications. The latter was seen to be furthering the pursuit of US interests in controlling trans-national optic fibre networks and the communications hardware export industry (Hills 1986:195; Tunstall 1986:55).

Admittedly, government telecommunications and security policies are usually the eventual outcomes of mutually competing interests and even 'turf battles' (Pfaltzgraff 1984:297) that tend to give shape to legislative aspirations without considering their impact on disparate elements of the state's machinery (Pfaltzgraff 1984:292; Krasner 1978:passim; Jepperson *et al.* 1996:50ff). In this particular instance, what some policy makers perceived as economic security (see for instance UK Reference Services 1994:1) came into direct conflict with national security. Thus, capitalist restructuring in the field of telecommunications resulted in serious, destabilising repercussions to what the law enforcement community considers to be one of its most valued investigative weapons. Ultimately, in this case, the state's ability to access the patterns and content of citizens' communication has been seriously thwarted, not due to some lobbying onslaught by civil

[7] Although the DoD's lobbying convinced Ronald Reagan to create the presidential-level National Security Telecommunications Advisory Committee (NSTAC), which initially consisted of the heads of 27 telecommunications industry members and today continues to advise the US administration on security issues related to the creation of the NII.

liberties militants, nor due to carefully orchestrated sabotage by socially-minded computer hackers, but rather by the internal inconsistencies of government policy.

8.3.0. CI as a Feature of Digital Systems.

Undoubtedly, RIPA and CALEA represent concentrated attempts by law enforcement agencies to gain access to the design of public telecommunications networks, which has so far developed in the absence of collateral principles such as national security or law enforcement oversight. The shared ambition of RIPA and CALEA is to elevate the status of such principles to guiding parameters in the design of digital telecommunications networks –an attempt which has been described by observers as "forced integration of specific enhanced surveillance features into the nation's telecommunications infrastructure" (Dempsey 1998).

As shown in section 6.4.0, early indications suggest that the UK's RIPA interception model appears to favour the vision of a permanent interception presence built into the digital telecommunications network. Yet, even in the US, where advanced models of ISDN interception appear to be based on detachable wiretapping technology, industry representatives are detecting an element of technical permanence in CALEA blueprints, which they see as introducing "a surveillance functionality into the [...] switching fabric and into the logic" (Int16:229-230) of telecommunications networks.

An example illustrative of the above is the redesigning of all digital switches, which is a minimum requirement posed by both CALEA and RIPA. The US experience shows that carriers are willing and able to delay the redesigning of switching equipment on financial and administrative grounds. Yet it appears certain that the next generation of switches will come with standard ports specifically designated for CI (Int11:129-132; Int48:118-125; Blair *et al.* 1995). The eventual materialisation of this redesign will signify the first documented instance in which US and UK law enforcement and intelligence agencies will be permitted to have an input into the design process of public communications systems, equipment and, possibly, features (Int08:184ff; Clayton *et al.* 2000; Berman & Dempsey 1996; Anon 1999e)[8]. Thus, for the first time, there appears the very real

[8] It would be erroneous, however, to assume that law enforcement demanded and was refused access to the design of public telecommunications systems prior to digitisation. According to FBI policy advisors R. Boucher and D. Edwards, "until recently, the question of system design was never an issue for authorised surveillance, since intrinsic elements of wirelined networks presented access points where law enforcement, with minimum assistance from telephone companies, could isolate the communications associated with a particular surveillance target and effectuate an intercept" (Boucher & Edwards 1994).

possibility of the latter technologies being gradually transformed into a vehicle for the practical expression of law enforcement and intelligence management goals. In an important sense, therefore, the long-term outcome of this process is likely to produce a public telecommunications system architecture whose technical features will partially incorporate the operational principles of state-sponsored CI.

This is a recent and unprecedented development. Thus, understandably, the scant relevant literature has yet to take into account this apparent use of technological design as a means of furthering the political aspiration of UK and US intercepting agencies. Yet, under the light of the present research, it would appear that any future attempt to assess the social and political impact of digital CI would be lacking in analytical depth if it failed to take into account the sociotechnical particularities of the debate –that is, the interaction of political, social, financial and cultural constituencies that contribute to the meaning of a technological product[9].

8.3.1. The Fusion of Culture and Technology in CI.

A significant benefit of analysing digital CI under the prism of sociotechnical discourse is the systematic consideration of non-technological factors in the evaluation of CI developments. This, in turn, allows for a higher degree of flexibility in forecasting the trajectory of CI trends in an increasingly digitised and deregulated telecommunications environment. In other words, the realisation that strictly technological developments will not be decisive in determining the degree and extent of CI in the future is essential for an elaborate understanding of the phenomenon.

Digitisation is an illuminating case in point: regardless of whether digital telephony systems in the US and the UK will move toward a high-speed wireline or a satellite wireless system, increasing digitisation will continue to subvert CALEA or RIPA-based CI models. In this sense, at their present stage, neither CALEA nor RIPA are future-

[9] Well-qualified, though regrettably rare, examples of such a sociotechnical analysis of digital communications technology can be found in Clark *et al.* 1989, Molina 1990 and Mansell 1993, who states that "a political economy of network design must be implemented [with the aim] of exposing aspects of telecommunications network evolution that bias its development and become part of a complex system of institutionalised power relations [...]. The political economy of the telecommunication network will offer an analysis, which is complementary to related approaches to the relations of power and control that are embodied within the electronic communications environment. It should also focus on choices regarding the way in which network evolution influences calling patterns, privacy of customer information, and the centralisation or decentralisation of control over information conveyed, or generated by public network transactions" (ibid.:35).

proof or able to guarantee the exercise of state-sponsored CI in the digital telecommunications environment:

> with ISDN coming up, with fibre to the home, I mean, what are you going to do then? You can't go inside a person's home and run some beads out the back door, you know, into a recording device [USTA CALEA lobbyist and point person, Int16:32-34];

> with fibre-to-the-home [...] there's no switch point [...], there's no place to put [a wiretap]. Are you going to have [...] the government agency knock on your front door and say "I want to tap into your fibre system"? It [...] isn't going to happen. So, yes, I think there are more questions that are going to be asked and there are very few solutions that are going to come forward [Technical Director of a large US telecommunications association, Int17:208-215].

Fibre-to-the-home technology is but one potential element in the development of digitisation that has led many observers to doubt the technical feasibility of CI practices in the future. This, however, is not necessarily the case. It is certainly true that parts of CALEA and RIPA appear to have already been surpassed by technical developments, such as voice-over-IP[10]. However, this research has shown that ISDN, fibre optic and even packetised data-based interception are technically feasible either through bridges installed in local area networks (section 6.3.2), through IP detection and identification systems (section 6.3.4) or through traffic mediation and filtering (section 6.3.4). Yet another comprehensive CI scheme, which has never been publicly suggested, though it is technically entirely feasible, could involve the reconfiguration of the national telecommunications network's routing structure, so that it would become mandatory for all information transmitted through the network to pass through any one of a number of

[10] An interviewee specialising in US telecommunications legislation confided: "I think the interesting thing about legislation and regulation [...] in that sort of technology world is that technology is constantly outpacing regulations and legislation. And you can see with CALEA that [...] they never foresaw the [...] problems they're having with IT [(information technology)]. By the time the FCC gets a rule out on anything technology has already far surpassed it and it's already dated. I have this feeling that by the time all of this gets sorted out in the courts they're going to have a whole new set of questions to answer [...] as we have all this convergence going on in the industry" (Government Relations Director of a large US telecommunications association, Int18:75-181; see also Int19:531-532; Freeh 1997b). British interviewees were equally pessimistic about RIPA's prospects of endurance: "I think maybe in 10 years' time we'll need another R.I.P. Bill, which will kind of merge it, so that the whole thing becomes a bit more technology-neutral then" (Regulation Officer and law enforcement liaison of large ISP association, Int10:22-24); "there is a need to change all this, but then, the question arises 'well it's all going to change again [...] within the next 3 or 4 years [laughs]; how do you write legislation which has got to be future-proof, but is not just a blank cheque for the Secretary of State [...] to do what [s/]he feels like at the time?'" (British Telecom Regulation Affairs Officer, Int11:290-294); "there's nothing there behind [RIPA] on which we can put a yardstick and say 'yeah, that will actually sit on and stand the test of time'" (TUFF fraud liaison officer, Int12:297-298; see also Int04:265-267; Int04:267-272).

designated switching stations equipped with mediation and filtering devices.

Nevertheless, the fact that digitally enhanced models of CI are technically feasible does not mean that they will materialise. As shown in section 7.4.4, financial implications are likely to be of paramount importance for carriers when it comes to deciding on the particular features of digital CI implementation. In the words of an industry observer, "anything is technically feasible. [The question i]s at what price is it feasible and who's going to pay for it?" (Int7:160-161; see also Int01:349ff). Ultimately, the degree of realisation of governmental CI ambitions in the digital age will largely depend on the potential impact of these ambitions on the financial health of commercial carriers.

Additionally, this research suggests that cultural forces will also play a pivotal role in determining the limits of practicability in digital CI models. As explained in section 7.4.3, US and UK telecommunications market deregulation resulted to an unprecedented cultural shift in CSP corporate culture. Thus, although the new, private CSPs recognise the social significance of communications policing (section 7.1.0), they do not appear to share their predecessors' favourable attitude toward the operational mandates of UK and US law enforcement and intelligence agencies. What is more, as already discussed in chapters five and seven, the traditionally close relationship between UK and US law enforcement agencies and CSPs has taken shape largely in the shadows of legal accountability and is the informal product of complex political and administrative factors. Any efforts to restore this relationship would indeed benefit by operational proximity caused by legal norms. However, if historical precedents are to be decisive in this context, this restoration would have to take place mostly outside the realm of legal directives. Ultimately, it should be expected that, without the restoration of this relationship, the realisation of the full extent of RIPA and CALEA's ambitions in regards to CI will prove unattainable in the deregulated telecommunications environment.

To this extent, one of the primary ambitions of both RIPA and CALEA is to strengthen the institutional interface between law enforcement and the new, private telecommunications carriers –something which both industry and law enforcement representatives indicated in the context of this research (section 7.4.0). There are indeed signs that, under the new legislation, the relationship between the telecommunications industry and law enforcement will assume an increasingly more structured and defined

format. But it is still too early to draw conclusions on whether such signs are going to intensify in the future.

Finally, the practical extent of CI in the digital telecommunications environment will also depend on the legal response to technical innovation. Namely, it should be expected that the design and use by government of more aggressive CI techniques will be met with legal challenges by carriers and civil liberties watchdog groups –especially if the uses of these techniques appear to urge renegotiations of already enacted privacy and human rights legislation. The case of Carnivore should be viewed as indicative of this potential (Dorobek 2001; Schwartz 2000). In turn, the outcome of any future legal challenges will greatly depend on the contemporary political climate that will permeate national and international relations. Events that occurred in the context the Cold War or domestic paramilitary activity –examples of which are the Vietnam war and the Oklahoma bombing in the US, as well as the Northern Irish dispute in the UK– have in the past triggered more aggressive uses of UK and US state-sponsored CI (Anon 1996b; Dillon 1999). What is more, as shown in section 7.5.9, US law enforcement agencies have been shown to be prone to the use of selective criminal and political events to justify their CI requirements (Strum 1999). In this sense, one would have to conclude that the turn of events linked to the Northern Ireland peace process, the US's relations with Russia and China or the activities of paramilitary agents or groups within the US are inextricably linked with the future of CI in the two nations (see section 9.3.0).

8.4.0. Blackboxing the CI Debate.

There are few, if any, issues in the general debate on domestic CI that generate a genuine need for concealment. Although surprisingly few individuals are actively involved in the practice of CI[11], basic knowledge of telecommunications systems, as well as consultation of popular technical manuals are usually sufficient to familiarise one with the inner workings of CI models and techniques. In fact, even highly classified interception software and hardware, such as FBI's DragonWare, are admittedly by-products of commercially available monitoring tools, all of which are freely available to consumers (section 6.3.2n38). In the UK, law enforcement officials themselves recognise that

[11] Prior to the initiation of an interview conducted in the context of this project (Int21), the interviewee confided that there were fewer than a handful of individuals in all of BellSouth who even knew what CALEA stands for, let alone being actively involved in CALEA operations.

criminals wishing to evade law enforcement CI schemes are "already aware of what [law enforcement's] capabilities are" (Stoddart 1999).

Yet, despite that inevitable openness, or perhaps because of it, secrecy has been an indispensable component of both the UK and US CI debate (sections 7.5.1; 7.5.2) and there is evidence to suggest that it will continue to be so in the future (section 6.3.0n27). These findings appear to confirm the suggestions of the wider literature on the subject, which tends to view secrecy as an inherent feature of the culture of state-sponsored CI (section 2.2.2).

There is little doubt that security issues, such as state-sponsored CI, tend to be insulated from popular control and knowledge in representative democracies (Russett 1990:146; Int05:399-406; Int08:453-454; Int11:446-449). Nevertheless, no evidence has been found in the course of this research that would lead to an interpretation of secrecy as the primary, or even as a systematically planned, barrier to accountability and transparency over state-sponsored CI. To begin with, secrecy has not been unilaterally imposed upon the CI debate by the UK and US state apparatuses. In the course of this research, corporate attitudes to secrecy and concealment of CI issues have proved much more rigid and impenetrable than governmental attitudes on the subject. An indicative example is that, on both sides of the Atlantic, the ratio of interview requests to affirmative replies was much more positive in the case of government officials than in the case of corporate representatives. Furthermore, it has already been noted that, in the UK, CSPs were instrumental in establishing a veil of secrecy around the digital CI debate even prior to the emergence of IOCA (section 7.5.2)[12]. Eventually, this veil of 'confidentiality' was respected even by a number of civil liberties groups participating in negotiations over RIPA (Bowden 2000:296-300). Thus, by no means was secrecy a mandate imposed by a number of conspicuous governmental departments. Rather it was an all-embracing cultural attitude that has its roots in market competition[13] between carriers (section 7.5.4) as much as in enduring bureaucratic values that lie in the heart of the sovereign nation-state.

More importantly, the very fact that the present thesis has been accomplished testifies to the considerable amount of CI-related information that has been made publicly available

[12] When this was exposed, it caused a severe rift in relations between certain segments of the telecommunications industry and the civil liberties community (Int01:295-297).
[13] Which incorporates consumer notions such as commercial confidentiality.

by government agencies on both sides of the Atlantic. In fact, the degree of government openness over RIPA and CALEA has been unprecedented both in the UK –where until a few years ago government often denied even the existence of its co-operation with industry over CI (Int12:451-455)– and in the US –where the last major legislative CI reshuffle occurred during the peak of J. Edgar Hoover's dictatorial FBI reign, between 1967 and 1968. Indeed, it is apparent that the CI agenda of UK and US law enforcement and intelligence agencies has been widely advertised in the public domain, either deliberately[14] or through decisive document leaks, such as that of *Looking to the Future* in the UK. This latter restricted document, jointly drafted by associations representing the British intercepting agencies[15] and addressed to the Home Office, recognised that RIPA's CI requirements subvert human rights legislation sanctioned by Data Protection laws and the European Union (Gaspar 2000:§7.1.1) and yet refused to rewrite RIPA. Rather, it proposed further law enforcement and intelligence-friendly CI mandates, including a suggestion that all digital and analogue data "generated or routed through a CSP's network" at all times and by every user in the British Isles should be retained for a period of seven years (ibid.:§6.1ff). It also demanded that the UK government

> should be prepared to defend our position, accepting that once communications data has been used to satisfy the business needs of CSPs, retention is still vitally important to the Agencies and the Criminal Justice System [ibid.:7.1.3].

The document was leaked to the Observer newspaper (Ahmed 2000), where it made front-page news and generated numerous editorials in the British press. The fact that, despite the revelations of *Looking to the Future*, the RIP Bill was proposed and eventually enacted by the UK governing administration without causing widespread political turmoil among the British electorate is significant in its implications. It should lead researchers to question the simplistic view that information secrecy is what stands between the machinations of conspiratorial government bureaucrats and an ignorant yet volatile electorate, which is prepared to defend civil rights as soon as the latter appear to be threatened by the policy intentions of non-elected administrators. In the future, RIPA and CALEA are likely to restore and even reinforce the CI capabilities of centralised government institutions in the US and UK. If this does indeed occur, it will be largely

[14] Such as by the FBI's PR campaign to promote CALEA (see http://www.askcalea.com).
[15] ACPO, HM Customs and Excise, the Security Service, Secret Intelligence Service and GCHQ (Gaspar 2000:§1.1.1).

the outcome of a permissive social contract, in which few organised civil society groups have questioned the CI mandates of law enforcement agencies.

8.4.1. The Intelligence Element.

Equally few, if any, organised groups or individuals have questioned the CI mandates of UK and US intelligence agencies. It should be noted that, in public, both UK and US intelligence agencies have remained largely silent during the RIPA and CALEA debates. Two reasons could potentially explain this exclusion: (a) either commercial telecommunications carriers are more sympathetic to the mandates of intelligence agencies, as opposed to those of the law enforcement community; or (b) the intelligence community has in its disposal sophisticated CI technologies whose function does not require carrier assistance. It is possible that both (a) and (b) are partially true, though there is no evidence pointing toward (a). On the other hand, interviews conducted in the context of this research revealed significant evidence pointing to (b). Specifically, knowledgeable observers pointed out that carriers see little of intelligence operatives, who make use of CI instruments not usually available to law enforcement:

> [a]nd then [you have] your intelligence agencies, who…they just do whatever they want, anyway. I mean, often times they don't even involve carriers [CALEA Compliance Attorney, BellSouth USA, Int20:195-196];
>
> interception of communications [involves] technology that the police have no hands on, [no] ability with and no access to. I mean…obviously that doesn't go for the security services, because they're probably listening to this [laughs]. But, in the normal run of things […] they would be reliant on the […] operator [British Telecom Security Officer, Int07:260-265]
>
> GCHQ probably can do all this stuff. That's its job. But those sorts of resources are not available on a compartmentalised […] way for most areas of law enforcement [Bowden 2000:643-645];
>
> there are a number of reasons why you would carry out interception. The majority […] that BT is directly involved with is probably to do with crime. There are other reasons, you know, [such as] for national security and the economic wellbeing of the United Kingdom […]. And, those sorts of areas are […] the areas where GCHQ and other such government organisations carry out interception.
>
> **Q:** Without your co-operation?
>
> **A:** Possibly…yeah [British Telecom Regulation Affairs Officer, Int11:515-522];

> [c]an the [intercepting agencies] do it on their own? If the crime is serious enough, if it actually addresses issues such as national security, the chances are they can. [O]ne's only got to look at [...] things like the GCHQ set ups –you know. They [...]'re not playing games [.... B]ut those types of resources are very much at the very high sort of national security intelligence gathering level [Former Special Branch Officer, Int12:560-565].

8.4.2. Oratory and Dictionary CI Systems.

The speculative existence of large-scale CI resources that can be installed and function without the assistance and co-operation of CSPs has never been confirmed or disputed by active members of the UK or US intelligence agencies. The latter are usually unwilling to interact with representatives of civilian organisations or even with state officials who are not members of designated military, intelligence or national security committees (HCTISC 1999a; Tenet 2001). Recent research, however, suggests that both the NSA and GCHQ have the ability to intercept and collect verbal and non-verbal communications data transmitted through wireline and wireless systems in use today (Campbell 1999:3ff)[16]. Specifically, a series of investigations funded by the European Parliament in 1999 (ibid.) has unearthed the existence of a US and UK-sponsored powerful CI collection and analysis system by the name of Dictionary. According to Campbell,

> key component[s] of the [Echelon] system are local 'Dictionary' computers, which store an extensive database on specified targets, including names, topics of interest, addresses, telephone numbers and other selection criteria. Incoming messages are compared to these criteria; if a match is found, the raw intelligence is forwarded automatically. Dictionary computers are tasked with many thousands of different collection requirements, described as 'numbers' (four digit codes). Tasking and receiving intelligence from the Dictionaries involves processes familiar to anyone who has used the Internet. Dictionary sorting and selection can be compared to using search engines, which select web pages containing key words or terms and specifying relationships. The forwarding function of the Dictionary computers may be compared to email. When requested, the system will provide lists of communications matching each criterion for review, analysis "gisting" or forwarding [Campbell 1999:11-12].

Dictionary is originally a US technology. However, a 1991 *World in Action* UK television programme discovered two Dictionary systems at GCHQ's Westminster as

[16] The NSA-controlled system that performs these functions is widely known –though never acknowledged by the US authorities– as Echelon.

well as Cheltenham offices (ibid.), probably operating under UKUSA[17] alliance agreements. What is more, the programme revealed that, although installed and maintained by GCHQ, Dictionary computers were operated by British Telecom security-vetted staff.

The impressive component of Dictionary systems is not their interception function, but rather their filtering capacity, which appears to have virtually transformed the nature of intelligence-oriented information processing by filtering mass quantities of intercepted data and forwarding to intelligence gatherers only data that corresponds to a set of pre-programmed criteria. This feature significantly decreases time and monetary constraints that large-scale CI operations usually face.

Dictionary is generally believed only to be able to process non-verbal communication. Campbell reports that "effective voice wordspotting systems do not exist [and] are not in use, despite reports to the contrary" (Campbell 1999:13). However, information obtained in the course of the present thesis points to the possibility that new features developed in the context of another NSA-sponsored CI system, code-named Oratory[18], offer the ability to automatically filter and analyse verbal communications from a variety of transmission sources. According to the above information, which is exhibited in full in Appendix 4,

> Oratory works on three different levels. On the first level, it scans targeted voice communications and digitises them [...]. It then scans the digitised signal[s] and fishes out sounds that phonetically match [...] desired keywords [...]. Finally, some Oratory systems –the most advanced– can act as voice recognition systems and [...] can identify the person behind a voice. Then [Oratory] forwards that [analysed] information to Dictionary, which is nothing more than a user friendly search engine. [It has] helped us tremendously, mainly b[ecause] it can be portable. Its main component, which is tempest-proof[19] and contains demux and microwave converters, is only about as large as your average billfold. This means you can install [it] in a configured middle-of-the-range laptop and use it with an [e]xtension or a strong-encryption mobile phone from anywhere you want [Appendix 4].

---

[17] UKUSA is an intelligence collaboration agreement enacted in 1947 between the two nations. Australia, Canada and New Zealand later joined the agreement. UKUSA was only publicly acknowledged in 1999 (Campbell 1999).

[18] Oratory has been mentioned –but never elaborated on– by former CSE employee and NSA trainee Michael Frost. See Frost 1994:152; 1996 and Davies 1997)

[19] The term 'tempest-proof' describes electronic mechanisms which do not emit electromagnetic signals and therefore cannot be traced by electromagnetic detectors.

Evidently, the implications of the existence and use of such a capable and flexible CI technology could potentially be immense for domestic CI. Dictionary, Oracle and other similar CI systems were developed for use in the arena of international espionage, where legal guidelines and regulations are traditionally at a minimum or, when they exist, are rarely respected. Yet, a scenario where these systems would be used for domestic CI should not appear distant[20]. The NSA has admitted that intelligence on US citizens is often obtained "incidentally" in the course of CI operations (Bamford 1982:331), while the FBI has revealed that almost two thirds of all federal CI orders relate to national security, including counter-terrorism and foreign counterintelligence operations directed against US citizens (Freeh 1997a). The obvious question that arises is whether Oratory CI systems are used domestically in the US or in the UK for national security CI operations. What is more, in a potential situation where a CSP would be unwilling or unable to facilitate a law enforcement domestic CI request, would senior FBI or law enforcement officials with informal ties to the intelligence community be able to resist the temptation of using Oratory systems to accomplish their CI requirements?

The lack of official information about the existence of Oratory and other Echelon-based CI systems leaves little room for adequate regulation or oversight. In the absence of a rigid framework of accountability, the possibility for detecting and disciplining members of intelligence organisations who wish to operate outside legal norms are considerably limited. In 1996, for instance, Michael Frost, a former Canadian Security Establishment (CSE) official and NSA trainee revealed that

> [i]n pursuit of plausible deniability, CSE, GCHQ, and NSA have repeatedly used each others' personnel and resources to evade laws against domestic spying [...].So, Canadians were [often] sent to conduct counter-espionage operations on US soil at US taxpayer expense so that [the] NSA could maintain deniability. In every way that counts, NSA broke US law and spied on its own citizens [Frost 1996].

In the same article, Frost describes how Margaret Thatcher invited Canadian and US intelligence officials to conduct espionage against two of her government's Ministers in

[20] Certainly, during the period of the Nixon administration, and through the Huston Plan, the American public came frighteningly close to being subjected to the same espionage techniques that the US uses against its foreign adversaries (Theoharis 1978). More recently, there have been cases of US citizens who, after filing FOIA requests, discovered records on their political activities created and maintained by the CIA (Tsang 1998). In addition, there are often pressures on the executive by members of the intelligence and military establishment to expand the domestic duties of intelligence agencies, including the CIA (Coryell 2001).

an attempt to acquire sensitive information without evading the law of the land (ibid.). These serious allegations by a former intelligence insider could well be fabricated, but the lack of even an official denial from the US or the UK security establishments hardly encourages well-intended speculators.

Ultimately, the intelligence dimension in the future of domestic CI should not be underestimated. Behind the scenes, members of the UK and US intelligence community, including military officials, have been particularly active in lobbying in favour of RIPA and CALEA. This surely suggests that there is a definite element of consistency and coherence between the digital CI goals of external intelligence and domestic law enforcement authorities on both sides of the Atlantic. Should developments permit it, this coherence may well increase to an unprecedented degree.

Chapter Nine

Communications Interception and Social Control in the Information Society

9.0.0. Introduction.

In chapter one, three introductory questions were posed as guiding parameters for the present research. The questions were: (1) what particular political visions do digital models of CI seem to favour and what do these visions appear to suggest for the future of citizens' privacy in the West? (2) What sociotechnical trends are evident today in information privacy policies in the UK and the US, in relation to CI? And (3) what is the potential importance of digital networking for practices of social management and control by governmental decision centres? These three questions will now be addressed in light of the preceding chapters.

9.1.0. The Political Visions Behind CI Legislation.

If we were to base our view of the history of UK and US telecommunications regulation solely on the existing relevant literature, we would have to infer that the impact on that history of issues around social control and national security has been minuscule. Chapter four of the present thesis demonstrates that, in many ways, this would be an unjustified inference. The political pursuit of social harmonisation and the drive to uphold the rule of law were certainly not the only influences on the formation of telecommunications policy; yet their role was anything but trivial and often helped shape the state's administrative perspective on telegraphy and early telephony.

These influences have not been abandoned following the epic passage from electric to electronic modes of communication. They are very much alive today, in what is often called the era of the information society. Their presence informs recently enacted legislation, which strives to discredit the popularised myth that decentralised digital communications networks, on which the information society concept is based, are inherently uncontrollable by governmental entities (King 1984; Masuda 1981; Horner 1996; Negroponte 1995). RIPA and CALEA are characteristic examples of such efforts inasmuch as they aim to secure the residence of law enforcement and national security mandates in the domicile of digital telecommunications policy.

Nevertheless, it should not be assumed that the conception, emergence and implementation of RIPA and CALEA were in any sense straightforward, delineated processes. The fact that both pieces of legislation were enacted *following* the standardisation and implementation of consumer-oriented telecommunications services attests to the exclusion of law enforcement and security agencies from these processes. Instead, both in the US and the UK, the telecommunications digitisation debate was observed and steered by financial-oriented state agencies whose priority was to safeguard and promote the competitive nature of the market, rather than to enhance, or even maintain, the social control capabilities of the state apparatus. It was only at a much later stage that law enforcement and security officials within the nation state were able to exercise the degree of influence that was necessary to alter the course of the state's telecommunications policy and steer it to a more security-oriented direction. In both cases, therefore, the state emerges not as a unified and monolithic decision-making mechanism, but rather as a site of struggle between plural forces with unequal and competitive access to state decision-making and planning.

The above assertion, however, should not lead to a view of the US and UK national security communities as isolated from state structures in representative democracies. In an important sense, the often aggressive promotion by state officials of measures proposed in RIPA and CALEA manifests the ideological and functional proximity between executive decision-making on the political level and the law enforcement and intelligence establishment in representative democracies. Particularly in the context of the UK's RIPA debate, telecommunications industry and civil liberties observers appear to have been overwhelmed in confronting political decision networks that are often

detached from mundane economic dilemmas and operate on a level exclusively occupied by national security priorities and concerns (section 7.5.8):

> whether you're talking about the interception of communications or acquisition of communications data or decryption powers or oversight or whether you're talking about the boundaries between those or whether you're talking within those fields themselves –wherever there's been a benefit of doubt or some leap that's got to be made to bridge the old regime and the new regime, the benefit of doubt has gone to law enforcement [...] to a quite astonishing extent, throughout the [RIP] Bill [Bowden 2000:67-72, 186; see also Hall *et al.* 1999].

There is little doubt that, both in the UK and the US, law enforcement and intelligence institutions used their position as members of the state apparatus to engage in what is often called 'direct lobbying' (sections 7.5.8; 7.5.9) –that is, lobbying directed at members of the executive cabinet and departmental officialdom (Shaiko 1998:261)[1]. Despite their systematic lobbying efforts, however, the vocal and traditionally powerful US law enforcement and security community has been unable to have CALEA implemented, almost eight years following its enactment. Resistance to the legislation by the telecommunications industry and its political allies has been impressive and unprecedented and has seriously threatened with extinction law enforcement's CI capabilities. There is no evidence that the UK law enforcement community's drive toward a CI-friendly telecommunications environment will be more expeditious: even though almost a year and a half has passed since RIPA's enactment, technical CI standards have yet to emerge from ongoing negotiations between industry and government (section 6.3.0).

These administrative impediments attest to the existence of an intricate labyrinth –a complex network of actors– standing between the adoption of national security directives by the state's executive machinery and their eventual application in a highly deregulated, competitive and evolving industry. What used to be a relatively closed sociotechnical constituency has now burst open and has been subjected to the eventful arrival of new entrants, characterised by different administrative priorities and cultural norms. The degree of conflict –or, perhaps, the degree to which conflict is visible to external observers– has thus increased and in doing so has further destabilised the formation of CI policy.

---

[1] For a sophisticated exposition of access as a parameter of effective lobbying see Truman (1958). In it, Truman remarks that an interest group remains essentially powerless unless it can gain and retain access to key niches within the government (ibid.:321).

9.2.0. Sociotechnical Trends in CI.

The complexity of this labyrinth has significant implications for the future of state-sponsored CI as a concept and practice. It means that the technological dimensions of CI in the digital environment will not determine the extent or nature of its use. In the UK and the US, CSPs are certain that the technical reconfiguration of their network, as required by RIPA and CALEA, will result in an inevitable increase in the volume of intercepted traffic (Int18:57-46; Int20:232-237; Anon 1999b; Dempsey 1995; O'Doud, 1999; Anon 1997a; Leahy 1999). In the US, where CALEA's technical standards have been unveiled, CSPs privately describe the potential volume of intercept requests as "huge", "unreasonable" and "astronomical" (Auble & Bender 2000)[2]. Indeed, the technological suggestions underpinning RIPA and CALEA appear to vindicate such expectations: the permanent hardwiring of interception capabilities into digital switching technology will undoubtedly be a challenging task because of the sheer number of switches that will have to be modified and replaced. However, once this task is completed, the permanent presence in the network, as well as the digitisation, of CI techniques are likely to reduce the financial cost of CI operations: the need to dispatch government agents out into the field to install wiretaps will be eliminated; the interception and collection functions of CI practices will be simplified; and the processing of intercepted data will be automated, possibly down to the transcription of oral communications (Int20:237-240).

Nevertheless, as explained earlier in section 8.3.1, a host of non-technical factors will ultimately determine the extent to which technical CI ambitions will materialise. The financial implications of CI are of primary importance for industry actors operating in a deregulated market environment. Competitive-oriented carriers are not willing to cover the cost of CI modifications and law enforcement agencies will have to lobby political decision centres requesting the allocation of extensive financial resources. Additionally, it could take years, possibly even decades, until the cultural relations between the new, privately-owned CSPs and law enforcement agencies are strengthened enough to accommodate the full extent of RIPA and CALEA's mandates.

[2] Thomas Wheeler, President of the USCTIA, once said in regards to CALEA: "[a]ll we wanted was to move from a propeller-driven aeroplane to a jet aeroplane, but the FBI wants to build the Apollo program[me]" (ctd in Vesely 1997).

Essentially, the answer to the question of whether state-sponsored CI will be enhanced in the digital environment is twofold. If enhanced CI is defined as the construction and application of technical systems that are able to intercept, collect, store and analyse information in a more intrusive, detailed and timely fashion, then the state's ability to intercept should be expected to increase by virtue of digitisation. If, on the other hand, enhanced CI is defined as the ability of organised government to secure: (a) a continual and effective technical interface with intelligent communications networks, which are owned by private corporations and whose technical features constantly evolve; and (b) the establishment and maintenance of consensus among disparate non-governmental actors in accepting law enforcement and national security mandates underpinning CI policy, then the state's ability to intercept in the digital, deregulated telecommunications environment is currently facing a crisis of unprecedented proportions.

This should ultimately lead us to the broader observation that the social shaping of technology does not necessarily imply a smooth and horizontal set of relationships between existing or emerging social values and the process of technological design. As new technological paradigms emerge, they are drawn into the arena of political negotiation and become subject to a host of contradictory requirements by disparate actors. The nature of these requirements is formed by the actors' perception of the challenges that new technologies pose for their particular interests, commitments and goals, which are often contradictory to those of other actors. Inevitably, the nature and extent of digital CI should be expected to evolve in relation to these contradictory forces.

9.3.0. CI and Social Control in the Information Society.

Ultimately, the legislative framework of CI is relative[3] and its interpretation over time will be highly dependent on the political challenges posed by intra-national and international relations. Numerous observers have noted that both CALEA and RIPA are vague and fail to define important expressions and terms mentioned in them, such as 'public telecommunications network', 'carrier' and 'reasonable intercept capability' (Int05:670-678[4]; Int10:191-197; Int12:293ff; Int20:96-200; Berman & Dempsey 1996).

[3] An FBI Special Agent characteristically remarked that "CALEA [...] is sort of like the Bible: every time you read it you can see something new in it –a new interpretation" (Int19:750-752).

[4] "Now, admittedly, the Bill talks about a reasonable intercept capability. But, clearly, what makes CSPs nervous is that what is deemed reasonable is entirely within the discretion of the Secretary of State at the time. And the only way to challenge that is through judicial review, which is [...] not very reassuring. Now, of course, the Home Office says 'well, why would we impose unreasonable requirements on the industry? [T]hat [woul]d be a crazy thing for us to do'. Well, I think that's not [a] particularly reassuring response [...] because [...] it's simply saying 'trust us not [...] to act stupidly'. Well, there's plenty of evidence of the government acting stupidly in the past, in this area and in other areas" (Bowden 2000:670-678).

Nevertheless, according to law enforcement officials, this legislative vagueness is not a conceptual failure, but rather a strategic omission, which is intended to decrease the possibility of the legislation having to be modified –or even possibly replaced– as various technical, social and political conditions change:

> there should be no restrictions placed on the scope and type of communication services which are subject to interception legislation. If exemptions are made, then the criminal will exploit them. By leaving the legislation wide, future developments and innovation will fall under the legislation [Todd 1999].

This can be taken to imply that the meaning of expressions such as 'reasonable intercept capability' is to be interpreted according to the immediacy of perceived threats to the social stability, economic wellbeing and defence security of the nation state. Chapter five of the present thesis explained that, during the Cold War, the extent of legal and illegal state-sponsored CI increased as panic over the activities of real or imagined internal adversaries overtook governmental administrations in the UK and the US. Admittedly, there has been little consideration in the debate over digital CI of this vital link between citizens' privacy and socio-political stability in the parliamentary democratic context:

> even if we trust the current government that doesn't necessarily mean that we will trust all future governments. I mean, MI5 in the past monitored Jack Straw [and other members of] Parliament. Phones were listened to on a regular basis. So, the government should be very careful and think twice before passing [this] piece of legislation [...]. Today we have the Labour government [..]; tomorrow [...] Tony Blair might be target of this sort of surveillance [Akdeniz 2000:227-234];

> each successive generation says "ah, yes, well that was in the past, that was 20 years ago, of course things are not done in that way right now". But I think one really has to view this approach with some scepticism and question the assurances that one gets today. [One ought] to worry about how these powers could develop in the future or how they could be abused by a more extreme government [Bowden 2000:273-275, 384-385].

The pillars of socio-political stability in the West are not as sturdy as they are often perceived to be. As this thesis is being edited for submission, the US has suffered the most lethal paramilitary attack on its territory in modern history. Militant cells have hijacked passenger aeroplanes and have used them to destroy US military and financial targets in Washington, DC, and in New York City's Manhattan Island[5], resulting in the

[5] On Tuesday, 11 September 2001.

deaths of many thousands and the severe disruption in all areas of civilian life in the country. As the US and many of its NATO allies are gearing up for the 21st century's first war, the effects of this dramatic incident on civil liberties have yet to be evaluated. Already, less than 72 hours following the attack, an unprecedented increase in the degree of state-sponsored CI has been reported in the US, as law enforcement and intelligence agencies are searching for the perpetrators behind the attack (McCullagh 2001; Lemos 2001). Additionally, in response to the attack, the US House of Representatives has approved a rapidly-drafted Bill[6] expanding CI legislation to cover "investigations of acts of terrorism" and "all forms of computer-mediated communications", including those involving more than one states, with a single warrant (Holland 2001). In essence, some of the more highly contested legal aspects of digital CI have been resolved literally overnight. If these late developments prove to be indicative of a rapidly changing political environment in the West, then a much more aggressive and forceful interpretation by state agencies of RIPA and CALEA's mandates is to be expected.

9.4.0. Suggestions for Further Research.

In addition to the above conclusions, the present thesis demonstrates that governmental and corporate secrecy over CI is not a valid justification for the widespread absence of vital social and political research on the field. Persistence and networking on behalf of researchers can penetrate the mistrust that government and industry security officials have of external observers, including academics. Undoubtedly, the issue is very polarised between security-oriented agents, consumer-oriented professionals and civil liberties-oriented activists, yet this should not be seen as a negative element from the viewpoint of research. The lack of substantial agreement in the debate often generates frustration among actors, which in turn makes members of every side in the debate wish to communicate their own story.

Neither should the unfinished status of digital CI legislation frighten researchers off the field. On the contrary, it should attract them to it. The incompleteness of the debate offers a unique opportunity for interested observers to glimpse into the chaotic construction site that is the process of sociotechnical negotiation between an array of often adversary actors. Usually, once the debate has been concluded and the negotiation

[6] Bill HR2500.

process subsided, the polished façades of industry's PR exercises and government's political rhetoric tend to deflect academic interest and curiosity. Researchers then have to engage into a sort of archaeological excavation of the debate, which is usually much more laborious than having had the luxury of witnessing policy formation.

One such archaeological excavation is required to address the gaps in our knowledge of the history of government telecommunications regulation, as well as of the history of CI in the UK and the US. In the case of the former, the role of social control concerns over telecommunications policy is totally absent from the literature, which has tended to reduce government regulation into a purely economic process. In the case of the latter, although CI use and abuse has been aptly documented –though in most cases not by academic researchers– the scant literature on the subject tends to analyse issues around the use of CI and other forms of state-sponsored surveillance as linear and conflict-free elements in social control. Surprisingly little attention has been given to issues of power, adversity and negotiation between government and industry actors involved in the conception, implementation and application of state-sponsored surveillance. The exposure of conflict in contemporary debates over digital CI should not necessarily be viewed as a recent phenomenon. On the contrary, it should be assumed that many historical accounts of the practice have failed to expose and draw attention to the inner complexity of the debate, which has probably characterised CI ever since the beginnings of electric telegraphy.

The future of digital CI is also worthy of researchers' attention: if the fragmentation of the telecommunications sector continues under deregulation, then the rising numbers of participants involved in the CI debate should be expected to impend tendencies by government and industry to monopolise and withhold relevant information. Thus, as the debate over state-sponsored CI opens up to public scrutiny, the role of social and political research should be to deconstruct issues of trust between civil society and government, as well as evaluate the impact of that trust –or lack thereof– on emerging models of citizens' privacy. If, on the other hand, the fragmentation of the telecommunications sector is overtaken by oligopolistic tendencies in the absence of state interference, then the potential of the debate being blackboxed will increase. Faced with such prospects, academic research will have to become more inquisitive and demand access to elements of the CI debate that are kept beyond the reach of public scrutiny.

Nevertheless, regardless of the long-term prospects of capitalist restructuring, future research on CI should consistently engage with the issue of governmental regulation of telecommunications and its impact on citizens' privacy. Undoubtedly, policy-makers in support of RIPA and CALEA view the concept of state-sponsored CI as an instance of vital social regulation. In other words, both pieces of legislation are intended to safeguard interests, which are perceived as socially necessary, but which the profit-oriented telecommunications market cannot be expected to meet voluntarily (Hills 1986:29; Int19:220ff). Yet, the financial impact of RIPA and CALEA, especially on smaller CSPs, cannot be overlooked. Interviews conducted in the context of the present research reveal a consistent concern among observers that small-sized CSPs will be unable to withstand the financial requisites of CI legislation:

> [large CSPs] have such tremendous resources, whereas smaller companies don't have the resources [.... CALEA requirements go] far beyond the capabilities of the small companies to [...] deal with this. All of the networking and the aggregation of [...] the data redistribution and the single point [...]–that's just [...] a level way above what these small companies that we represent would ever be capable of doing. So [...] there's surely a problem with small companies having this imposed on them for [...] no reason [Technical Director of a US telecommunications association representing more than 500 small-sized member companies, Int17:77-84];

> I think [...] there will be more major [industry] players in the future, rather than small-scale CSPs. Th[e latter] will probably die in the [...] light of these new developments, like the RIP Bill [...]. It's becoming a complex business to be [...] a CSP or run a CSP without be[ing] hassled by [...] law enforcement people [Akdeniz 2000:450-455; see also Int07:61-62; Virgo 1999; Clayton *et al.* 2000].

These warnings are not unfounded. The financial impact of CI regulations could potentially contribute to the elimination of competition in the deregulated telecommunications environment, thus gradually turning the market toward an oligopolistic direction, which, as explained above, would in turn blackbox the CI debate. Future research should therefore explore the state's intentions behind the proposition of digital CI legislation. In doing so, it should examine the extent to which RIPA and CALEA are partially being used by elements within the US and UK state apparatus as deliberate instruments of policy in an orchestrated attempt to shrink the multitude of industry actors involved in the CI debate (Bowden 2000:678-684).

In essence, none of the above suggestions for further research can even begin to be

addressed unless social and political researchers systematically turn their attention toward CI and other forms of state-sponsored surveillance. It is true that, especially in its domestic form, surveillance has traditionally been a politically charged area for academic research. It is an uncomfortable subject matter that becomes even more unpleasant when discussed in the context of parliamentary democracy, since it is not possible to consider it in depth without somehow stripping Western governance systems of their popularised democratic pedigree. This, however, is hardly an adequate justification for the self-imposed isolation of social and political research from the concept and practices of surveillance. This isolation has undermined attempts to adequately comprehend the nature and inner workings of governance in the West. During the Cold War it helped create the illusion among many academics that the structure of our communications systems was somehow unconstrained by institutional manipulation and control (Frey 1973; Almond 1960; Pye 1963); while during the rise of digital networking it contributed to popularised 'feel-good' analyses, produced with minimal reference to concepts of power and authority in technologically advanced social systems (Toffler 1980; Negroponte 1995).

And yet, the technological sophistication of the information society does not remove it from the functional characteristics of preceding modes of social development: there still exist social classes, centralised governing bodies, wars and mass movements. What is more, the networks of communication through which power is negotiated on a daily basis in advanced societies are not neutral. They embody technical visions of the political order in which we live. Sociologists and political researchers cannot afford to ignore these visions any more than an architect can ignore the density of the soil base on which a building is to be erected. When this is fully understood, we can perhaps begin to deconstruct the present realities, as well as the unfolding futures, of the information society.

SUPPLEMENTARY APPENDICES

Appendix 1: Sample Interview Questionnaire

Interview with Mr

Unit Chief
Telecommunications Industry Liaison Unit
CALEA Implementation Section
Federal Bureau of Investigation

Atlanta, Georgia, Wednesday 15 November 2000

Section 01: Defining the Context of the Interview

(a) I am Joseph Fitsanakis, and I am conducting this interview in the context of my doctoral research, under the auspices of the Department of Politics of the University of Edinburgh.

(b) In the part of my study that this interview relates to, I focus on the experience Part of individuals who are, or have been instrumental in orchestrating and overseeing the implementation C.A.L.E.A.

(c) I decided to approach you for interviewing because I am interested in the opinions of law enforcement bodies, such as the FBI.

(d) Confidentiality and Agreement.

(e) Recording the interview.

Section 02: The Implementation of CALEA

Question 01A: Allow me to start by going back a few years; it is my impression that CALEA was implemented back in 1994, that is, 6 years ago. Were you involved with telecommunications surveillance and relevant issues back then and even before that time?

- **if *'yes'*:** So you have been here from the start, as it were? Q.01B

- **if *'no'*:** So, CALEA had already been implemented when you entered this Q.01C profession?

Question 02A: From what you can remember, to what extent was there a feeling among law enforcement circles in America that CALEA was long overdue?

- **if 'large':** Why did it take so long for the legislation to catch up with changes in Q.02B telecommunications technology?

- **if 'small':** Was it a development that followed extensive preparation on behalf of law Q.02C enforcement lobbyists, or was it maybe the natural and expected updated version of already existing legislation that seemed inadequate in the digital communications environment?

Section 03: The Argument of CALEA

Question 03A: I have been looking at CALEA for some time now, and it seems to me that the 'juice' of the legislation can be somewhat summarised in the following way: "communications networks are, in a sense, public spaces, where people meet and interact. And, as is the case with all public spaces, law enforcement wishes to have a presence there —it wishes to be able to police them. Therefore, law enforcement wants to ensure that it has access to these networks, and CALEA is a way of doing that. CALEA is therefore a demand put forward to communications providers, asking them to make sure that law enforcement has an adequate presence in communications networks". Do you think that this a more or less accurate statement in regards to CALEA?

- **if '*yes*':** Q.03B Is this how CALEA is more or less perceived by the law enforcement community?
- **if '*no*':** Q.03C What would be a more accurate statement?

Question 04A: How important is communications interception as a weapon of law enforcement against crime in America today? What would it mean for law enforcement if it suddenly lost all legal access to the content of telephonic communications?

Section 04: Law Enforcement's General View on CALEA

Question 05A: Do you think that this request, as represented by CALEA, is a reasonable one?

- **Q.05B:** Would this also be the general consensus among the American law enforcement industry?

Question 06A: Is there such thing as a 'general consensus' among the ranks of the American law enforcement industry in regards to telecommunication surveillance? [From the outside it sounds pretty uniform, but is that really the case?].

- **if '*yes*':** Q.06B Can you then briefly convey to me the general consensus within the law enforcement community, in regards to CALEA?
- **if '*no*':** Q.06C Can you give me a specific example of that lack of consensus, in regards to CALEA?

Question 07A: One of the more interesting things that has come up during my research in the USA is that there some sort of a split between federal and local law enforcement agencies in regards to CALEA. Local law enforcement agencies don't see as much need for increased telecommunications surveillance quotas as do the larger federal agencies, probably because they don't make as much use of it. From your experience, would you say that this is correct?

Section 05: CSPs and the Consultation Process on CALEA

Question 08A: To what extent do you think that law enforcement [including the FBI] were able to be heard by the US government during the drafting process of CALEA?

- **Q.08B:** Why was that the case, do you think?

Question 09A: While talking to CSPs in the UK, about the RIP Act, [the British version of CALEA], I was told that law enforcement and intelligence organisations were in a better position to influence the government, than were other concerned actors, because they operate from within, and as part of, the government. Did that apply here in the US, in the case of CALEA, according to your opinion?

- **Q.09B:** Why is that the case, do you think?

Question 10A: Do you think that, when it comes to CALEA and communications interception in general, the law enforcement and intelligence communities still retain today considerable influence within the US lawmakers and legislators?

Question 11A: How does that influence compare today to that of CSPs over the government?

Question 12A: How does that influence compare today to that of the civil liberties lobby over the government?

Question 13A: To what extent has the element of trust been present in negotiations between law enforcement and CSPs in regards to CALEA?

Section 06: USTA's Lawsuit Against the FBI over CALEA

Question 14A: Mr , if I am not mistaken the USTA has actually filed a lawsuit against the FBI over CALEA, about a year ago, claiming that the rules that the FBI has set out as part of CALEA are "arbitrary, capricious, an abuse of discretion, and contrary to law and exceed the FBI's statutory authority". These are strong words, aren't they?

- **Q.14B:** Why do you think did the USTA proceed to sue the FBI over CALEA?
- **Q.14C:** What do you think does the USTA hope to succeed through this lawsuit?
- **Q.14D:** In your opinion, Mr , how significant, or noteworthy is the fact that the USTA has actually filed a lawsuit against the FBI over CALEA? What does it mean for the relationship between CSPs and law enforcement in the digital era?

Section 07: Life Under CALEA

Question 15A: According to your experience in the FBI, how has life been under CALEA? What has its impact been on the daily practices and the general standing of

smaller telecoms around the country?

Question 16A: It has been my impression that the gist of the industry's objections against CALEA is twofold: one side is financial —namely that the government and the FBI expect the industry to fit most of the bill incurred by the implementation of CALEA— and the other is technical —namely that some of CALEA's requirements are simply unrealistic from a technical viewpoint. What is your take on these issues?

- **Q.16B:** To what extent is CALEA proving to be technically feasible?

Question 17A: Do you see CALEA as, in a sense, allocating part of the law enforcement's workload on CSPs?

Question 18A: Is it your opinion that CALEA safeguards the privacy of citizens? In the long run, will it help to reduce, or even eliminate, the possibility of unlawful communications interception by third parties, including law enforcement and intelligence?

- **if 'no':** Q.18B Do you think that unlawful communications interception might go on in the future, perhaps even as a result of CALEA?

Section 08: Relations Between CSPs and Law Enforcement

Question 19A: Another area in which I am interested, is the impact that CALEA has had on the relationship between law enforcement and CSPs. Let me, therefore, ask you, how would you describe the relations between the FBI and the CSP industry today?

Question 20A: I was often told during my research interviews in the UK, that telecoms companies use interception assistance to law enforcement as a means of networking with them, in the hope that they will in turn receive help from law enforcement in the area of telecommunications fraud, a damaging phenomenon which is becoming increasingly extensive. Would this apply to this side of the Atlantic?

Question 21A: Are there today any areas of co-operation between the law enforcement community and the CSP industry [common training schemes, conferences, or meetings]?

Question 22A: Do you feel that, in this sense, CALEA somewhat normalises and strengthens the relationship between law enforcement organisations and CSPs?

Section 09: Police Reliance on ISPs Under the R.I.P. Bill

Question 23A: Do you think that the multiplication in the sheer number of communication service providers over the past few years has created problems for law enforcement wishing to contact those providers for assistance during interception operations?

- **if '*no*':** Q.23B Do you think that the relations between law enforcement and the new generation service providers have been similar in nature to their relations with the one and only provider, back in the monopoly days of telecommunications in the United States?

- **if '*yes*':** Can you give me examples of situations where these problems have arisen? Q.23C

  - **Q.23D:** What do you think are the reasons that have generated such problems?

Question 24A: Could the days of AT&T be described as 'the good old days' of communication surveillance when compared to today?

Question 25A: According to your personal knowledge, have there ever been cases in the US of CSPs refusing to assist law enforcement during a surveillance operation prior to the enactment of CALEA?

Question 26A: According to your personal knowledge, have there ever been cases in the US of CSPs refusing to assist law enforcement during a surveillance operation following the enactment of CALEA?

Question 27A: To what extent do law enforcement officers depend on the communication service provider, for achieving their communications interception goals?

- **if '*not very*':** You mean that they have the means of achieving those targets without assistance from service providers? Q.28B

- **if '*very*':** Can you give me an example? Q29C

Question 30A: To what extent can law enforcement meet its telecommunications surveillance targets in the digital environment, without the conscientious of service providers?

Question 31A: Does this increasing reliance of law enforcement on service providers make you nervous?

- **if '*yes*':** Why does it make you nervous? Q.31B

- **if '*no*':** Do you think that the industry has the necessary skills and experience to handle the sensitive nature of CALEA functions? Q.31C

Question 32A: Do you think it makes them nervous? Is CALEA a responsibility that they could do without?

Question 33A: How eager, would you say, are CSPs to assist law enforcement in its fight against crime?

Section 10: The Future

Question 34A: Is CALEA bearing fruit for law enforcement?

Question 35A: Having had the experience of 6 years under CALEA, would you say that the legislation was a wise and positive step forward?

Question 36A: How do you foresee the future of CALEA?

Thank you very much for your time

Appendix 2. The Inadequacy of Statutory Controls Over ICI.

Methods of surreptitious surveillance, such as telephone wiretapping, are regarded and treated by law as invasions of privacy, similar to a search of premises (Lambert 1986:207). This is indeed the reason for the requirement of a search warrant prior to a wiretapping operation. This is often condemned as improper by legal experts. The clandestine nature of wiretapping, it is claimed, makes it totally distinct from a conventional search of premises. The subject of a search of premise is, sooner or later, aware that his or her residence and personal effects are being searched. In the case of telephone surveillance, the subject is not shown the warrant while his or her personal conversations are being supervised and, usually, confiscated in the form of recordings. What is more, the subject is rarely notified of it, even if the investigation against him or her is, eventually, dropped. According to legal expert on wiretapping J.G. Carr (1998),

> [t]he unfortunate result is that persons whose conversations are overheard by electronic surveillance endure a more extensive intrusion into their privacy with fewer protections than persons subjected to a considerably more brief incursion during a conventional search of their person[al] effects [Carr 1998:§2.21].

Additionally, this "appalling invasion of privacy" (Maguire 1959:208), is often said to occur against all persons who telephonically communicate with the target of an investigation and have in many cases little or nothing to do with the investigation itself. A case in point concerns the wiretapping of public telephones. It is estimated that as many as half of all wiretapping operations involve the surveillance of one or more public telephones. During 1953, for instance, out of the 3,588 telephones wiretapped by the New York City Police Department, no fewer than 1,617 were public (Brenton 1964:158-159; Murphy 1965:150). In effect, during such operations, the conversations of every person who used –or was called by anyone using– those 1,617 telephones, were monitored. According to Carr (1998):

> [a]s conversations of unknown individuals are intercepted, the electronic surveillance resembles a random stop-and-search, without probable cause, of every person who appears in the company of some known person who is suspected of being involved in criminal activity. This approach [...] permits electronic searches of unknown persons on no basis other than conversational association [Carr 1998:§2.28-§2.29].

Nowhere in the 1968 Omnibus Crime Control and Safe Streets Act is this controversy addressed. In Britain, the 1957 *Birkett Commission* did consider, but ultimately

dismissed the issue by stating that:

> [t]he interference with the privacy of the ordinary law-abiding citizen of with his [or her] individual liberty is infinitesimal, and only arises as an inevitable incident of intercepting the communications of some wrongdoer. It has produced no harmful consequences [Command 283 1957:§8].

Another legal controversy is that of the interception of a telephone conversation under permission by the caller, which requires no warrant in Britain or America. In the US, the law assumes that the caller is the 'sender' of the message, and therefore the rightful owner. Yet, unlike a letter, the inevitably interactive character of a telephone conversation presupposes two senders of oral messages, each of whom generates part of the interaction (Maguire 1959:206). In Britain, the issue is not addressed by law, which states that the only rightful owner of messages transmitted telephonically is the service provider (Lambert 1986:209-210).

Spindel (1968:11) asserts that laws concerning telephone surveillance have ranged from inadequate and uncertain to confused and chaotic. To illustrate his point, he describes a number of legal case studies. In one of them, a US High Court defined a wiretap as presupposing a physical connection to a telephone line. Rather expectedly, local law enforcement agents resorted to the use of miniature induction coils, which can record telephone conversations without being in any way attached onto the telephone line (Spindel 1968:29). This characteristic lack of understanding of the technical complexities of wiretapping is accompanied by what many legal experts have described as "the peculiar wording" (Maguire 1959:211) of relevant legislation. In section 5.6. of Title III, for instance, the confusion over "interception and divulgence" is described. In that case, not only did federal officials interpret the legislation to mean that law enforcement agencies were allowed to wiretap as they pleased as long as they did not recite the content of telephone conversation in court[1], but the USDoJ went so far as to suggest that, if one officer performed the wiretapping and another divulged the content, then neither of the two was in violation of §605 (Carr 1998:§1.16).

Another controversial issue is the emergency clause[2] of the 1968 Omnibus Crime Control and Safe Streets Act, which allows unwarranted telephone surveillance during

[1] "Essentially, all Section 605 amounted to what was an instruction to the government that while wiretapping was fine, don't ever let anyone know that you've done it" (Gill 1994:7).
[2] §2518(7).

emergency situations. The term 'emergency' is not defined, thus, critics claim, inviting misinterpretation and abuse. As Michigan Democratic Senator P.A. Hart once remarked with regard to the term, "if one is a good policeman everything is an emergency to him" (ctd in Lapidus 1974:94).

Today it is widely accepted that there have indeed been instances when state officials deliberately and systematically misinterpreted the peculiar wording of wiretapping laws in order to evade the privacy of citizens. Such was the case with the 1940 Roosevelt directive, described in section 5.3.0. Roosevelt's intention was to use wiretapping as a means of detection of aliens, or Americans, who worked for foreign governments as spies, saboteurs and agitators. Yet, for more than 30 years, it was extended by the FBI to cover the illegal surveillance of left wing groups, civil rights campaigners and other domestic dissidents (Donner 1980:244; Jeffreys 1995:199-200). The FBI accomplished this by systematically externalising domestic dissidence and effectively viewing it as alien-motivated. As early as 1922, FBI General Director W.J. Burns[3] was convinced that

> [t]he Communist International at Moscow is directing activities in this country among [...] Negroes, labour unions and various social organisations including women's clubs and scouts [...] to undermine these organisations with the end of overthrowing the government of the United States and the establishment of the dictatorship of the proletariat [ctd in Lowenthal 1950:274-275].

A few years later, his successor, J.E. Hoover[4] was accusing the US Communist Labour Party of being "a gang of cut-throat aliens who have come to this country to overthrow the government by force" (ctd ibid.:41). Hoover centred his rhetoric on this 'foreign invasion' theme throughout his 48-year directorship of the Bureau. In 1938, he characteristically asserted that

> [s]ubversive alien theories and -isms are not only a drastic contrast to American ways of thinking, feeling and acting, but they stand for a complete overthrow of established ideals of American life and philosophy of government to which America is dedicated [...]. Our democratic institutions cannot exist half American and half alien in spirit. We are proud of our American form of government [ctd in Donner 1980:55].

The systematic externalisation of the American left enabled Hoover and the FBI to exercise surveillance over the movement under the defensive, patriotic and, most of all,

[3] Burns was Director of the FBI from 1921 to 1924.
[4] Hoover was Director of the FBI from 1924 until his death, in 1972.

legal, guise of counterintelligence. According to of F.J. Donner (1980:19), Director of the American Civil Liberties Union's Project on Political Surveillance, the externalisation of dissent served the FBI in its insistence that all its swords were shields.

Unauthorised wiretapping on national security[5] grounds was also consistently abused by American law enforcement agencies in their efforts to exercise domestic political intelligence over numerous Socialist Workers Party local candidates, as well as over the 1969 Chicago Seven, who, as analysts have shown, posed no threat to national security (Diffie & Landau 1998:173; Theoharis 1971:744). In 1986, the Socialist Workers Party sued the US government and the FBI for systematic violations of the constitutional rights of the Party and its members, which had lasted for over 20 years[6]. The Party won a total of US$263,500 in damages, which was subsequently paid to it by the FBI. During the Cold War, the FBI also used the 'national security' pretext to intercept the telephones of Martin Luther King Jr, the Southern Christian Leadership Conference, the Congress of Racial Equality, and the National Association for the Advancement of Coloured People (NAACP), even though all of them were firm advocates of non-violent approaches to demands for social equality (Diffie & Landau 1998:140; Donner 1980:244).

Arguably, the most notorious instance of misuse of the national security clause for purposes of political wiretapping occurred during the Watergate affair. In 1974, among the recorded conversations examined by the US House of Representatives Committee on the Judiciary, was the following extract from a March 1973 discussion between US President R.M. Nixon, presidential counsel J.W. Dean, and top presidential aide H.R. Haldeman. The three are discussing here how to justify their illegal wiretapping operations:

> **Dean:** You might, you might put it on a national security ground, basis, which it really, it was.
> **Haldeman:** It absolutely was.
> **Dean:** And just say that, uh...
> **President:** Yeah.
> **Dean:** ...that this is not, you know, this was...
> **President:** Not paid with CIA funds.
> **Dean:** Uh...
> **President:** No, seriously. National Security. We had to get information for national security grounds.
> **Dean:** Well, then the question is, why didn't the CIA do it or why didn't

[5] §2518(7).
[6] *Socialist Workers Party v Attorney General of the United States*, 73 Civ. 3160, 1986.

the FBI do it?
President: Because they were...we had to do it, we had to do it on a confidential basis.
Haldeman: Because we were checking them?
President: Neither could be trusted.
Haldeman: Well, I think...
President: That's the way I view it.
Haldeman: That has never been proven, there was reason to question their...
President: Yeah.
Haldeman: ...position.
President: You see, really, with the Bundy thing and everything coming out, the whole thing was national security.
Dean: I think we can probably get, get by on that [transcripts of the report of the United States House of Representatives Committee on the Judiciary 1975:243-234].

This is certainly not the only example of state officials who attempted to use the national security pretext to deliberately conceal their use of CI to protect their own, personal political interest; yet it is by far the most worrying, as it involved no other than the President of the US.

Appendix 3.0: Digital Telephony Features and Functions

The emergence of digital telephony has facilitated the introduction of hundreds of sophisticated specialized services. Many of these have presented substantial challenges to the ability of law enforcement and intelligence agencies to conduct authorised CI. The features or functions described below present the most significant such challenges:

Call Forwarding

Allows a subscriber to redirect the incoming calls by dialling the call forward activation code followed by the directory number to which the calls are to be forwarded. This feature can be activated and deactivated at any time from the subscriber's telephone set. Electronic switching systems have the ability to redirect an incoming call to either another directory number within the same exchange, or to another exchange over a trunk line. When a call is redirected by the switch, the call content is not transmitted to the subscriber's line, but instead is rerouted at the switch.

Speed Calling

Permits the subscriber to link a set of abbreviated directory numbers (i.e., one number or two-number sets on the telephone) to the directory numbers of frequently called parties at the subscriber's own initiative. This allows the subscriber to initiate a call by dialling the abbreviated one or two-digit number. Activation of Speed Calling is at the central office switch without involvement of the service provider. Some versions of speed dialling services permit the subscriber to change the assignment of directory numbers in real time, i.e., in the course of a call, or to change the number assignment remotely. Abbreviated Speed Calling codes created by the subscriber are accessible to law enforcement agencies from the local exchange carrier.

Three-Way Calling and Call Transfer

Enables a subscriber to add additional parties to a call that is in progress. When Three-Way Calling is invoked, the calling party or the called party temporarily suspends the

conversation, initiates service and connects to another party, then adds the new party to the initial call. Call Transfer behaves somewhat as Three-Way Calling, but it allows the initiator of the transfer to drop off the call while the remaining parties continue the conversation.

Custom Local Area Signalling Service (CLASS)

Is a set of call management features that provides the called party with control over incoming calls. CLASS features place more of the control of the call in the hands of the called and calling parties. Those features, which provide the called party more control, generally are enabled by passing the calling party's number to the terminating switch as part of the SS7 call setup message. About a dozen features are available through CLASS services. Automatic Recall allows the user to activate a procedure by dialling a code that automatically redials the last incoming call –whether or not the call was answered– without having to know the caller's number. Selective Call Forwarding enables a customer to define a list of telephone numbers and assign each a forward-to destination number. Incoming number on the list are forwarded to the assigned destination number. Selective Call Forwarding, and some of the other CLASS features, provide the customer with the ability to create, modify, activate, and deactivate screening lists at will without the involvement or knowledge of the service provider.

Number Portability

Number portability will allow telecommunications users to retain their telephone numbers over time, despite moving to different service areas and physical addresses. Potentially, users could be assigned a lifetime phone number. The telecommunications industry is also developing services that use a non-geographic number to identify a subscriber, such as AT&T's Follow Me service. Callers can be reached at the number regardless of their physical location or the type of terminal equipment used (i.e., home telephone, office telephone, cellular terminal). The infrastructure to support these types of services will be deployed over the next several years. The availability and use of portable and non-geographic numbers may have several implications for law enforcement. Law enforcement will have to be able to determine the carrier serving the investigation target, that person's

location, and any subsequent carriers and locations involved in transmitting the communication. Network-based capabilities to support lawfully authorized interceptions should be capable of providing dialled number information as well as translated numbers used by the network for routing calls to or from the intercept subject.

Integrated Services Digital Network (ISDN)

ISDN provides a broad range of voice, data, and image services based on digital communication for transport and control within the network. ISDN is based on combinations of 64 kbs (thousand bits per second) channels (lines) combined to increase bandwidth, and therefore increase the speed and capacity of transmission. Information is converted into digital form within the subscriber's equipment before being ported to the network. Since everything is in digital form, all voice and data information looks the same as it passes through the system. ISDN uses a separate 16 kbs digital channel (D-channel) for signalling, i.e., communication between the subscriber and the local switch. The D-channel is part of the access line, but it can be used to carry user-to-user information (e.g., packet messages) as well as signalling information. The subscriber controls the service features by sending messages to the switch, and the switch responds with messages to the subscriber over the D-channel. The functions and signalling for ISDN are processed through a number of standard interfaces that provide different data rates (i.e., speed and capacity). The two most common, and of most concern to the law enforcement agencies, are: (a) *Basic Access*: composed of two 64 kbs B-channels (for voice, data, or images) and one 16 kbs D-channel for signalling; and (b) *Primary Rate*: operates at a rate of 1.544 Mbs (million bits per second), composed of 23 B-channels of 64 kbs each, and one 16 kbs D-channel for signalling. With ISDN the subscriber's signals for activating or deactivating a feature is carried over a separate channel (D-channel) instead of being carried over the same channel as the call content. Traditional analogue intercept techniques are not compatible with ISDN.

Appendix 4

Subject: Re: Oratory?
Date: Mon, 10 Sep 2000 11:32:15 +0600
To: international@postmark.net
From: [redacted]
[Show Full Headers]

>
> What exactly is 'Oratory'? Is it part of Echelon, or part of
> anything at all? Does it recognise spoken keywords, or does
> it work like DCS in domestic operations?

Oratory was first developed about 12 years ago by a group of scientists working for the NSA at College Park. The project was supervized by DoDIIS Directorate and I believe two commercial companies helped with some modules and performance tests. It's a recent component (patented in US April 97) of a larger data collection/analysis system called Echelon II, as you know. Dictionary, which you mentioned last time, is a primary analysis component of Oratory.

Oaratory is made -- or was until last year though I don't think much has changed -- of about 33 supercomputers (not all the same kind or with the same capacities) interconnected in a platform along with 52 processing systems. One of these proecssing systems is Dictionary.

Oratory works on three different levels. On the first level it scans targeted voice communications and digitizes them, much like a mutlilevel quantizer. The communications have first been intercepted and magnetically stored for analysis. It then scans the digitized signal and fishes out sounds that phonetically match desired keywords. So it performs the automated signals selection, which is what Echelon II is all about. Finally, some Oratory systems -- the most advanced-- can act as voice recognition systems and if they have enough programmed information can identify the person behind a voice. Then, it forwards that information to Dictionary, which is nothing more than a user friendly search engine.

Something worht mentioning is that Oratory is still being worked on. It's got bugs and flaws. For instance it won't perform very well with certain accents like english spoken by heavily accented Chinese. It also wont work in high-volume traffic but only on targeted private networks inside intercepted high capacity. Also its voice recognition only does single voice prints. But even so it's helped us tremendously, mainly bcs it can be portable. Its main component, which is tempest-proof and contains demux and microwave converters, is only about as large as your average billfold. This means that you can install it in a configured middle-of-the-range laptop and use it with an xtension or a strong-encryption mobile phone from anywhere.

My team used it twice under pressure in Bangassou, Central African Rep. and once in Matale in Srilanka and every time results were outstanding. I know Oratory is now in use in east Asia and in the Balkans but I don't know how well it's performing.

I hope this helps

[redacted]

PGP RSA 1024 bit public key ID: 0x03341005. Fingerprint: 9E 14 FB 2A 34 96 24 37 98 A2 E0 D1 34 13 49 07 PGP DSS/DH 1094/3071 public key ID: 0x899DD4FF. Fingerprint: 5248 1320 B41E 83FC 1E8B A9E6 0922 AE66 897D D7FF

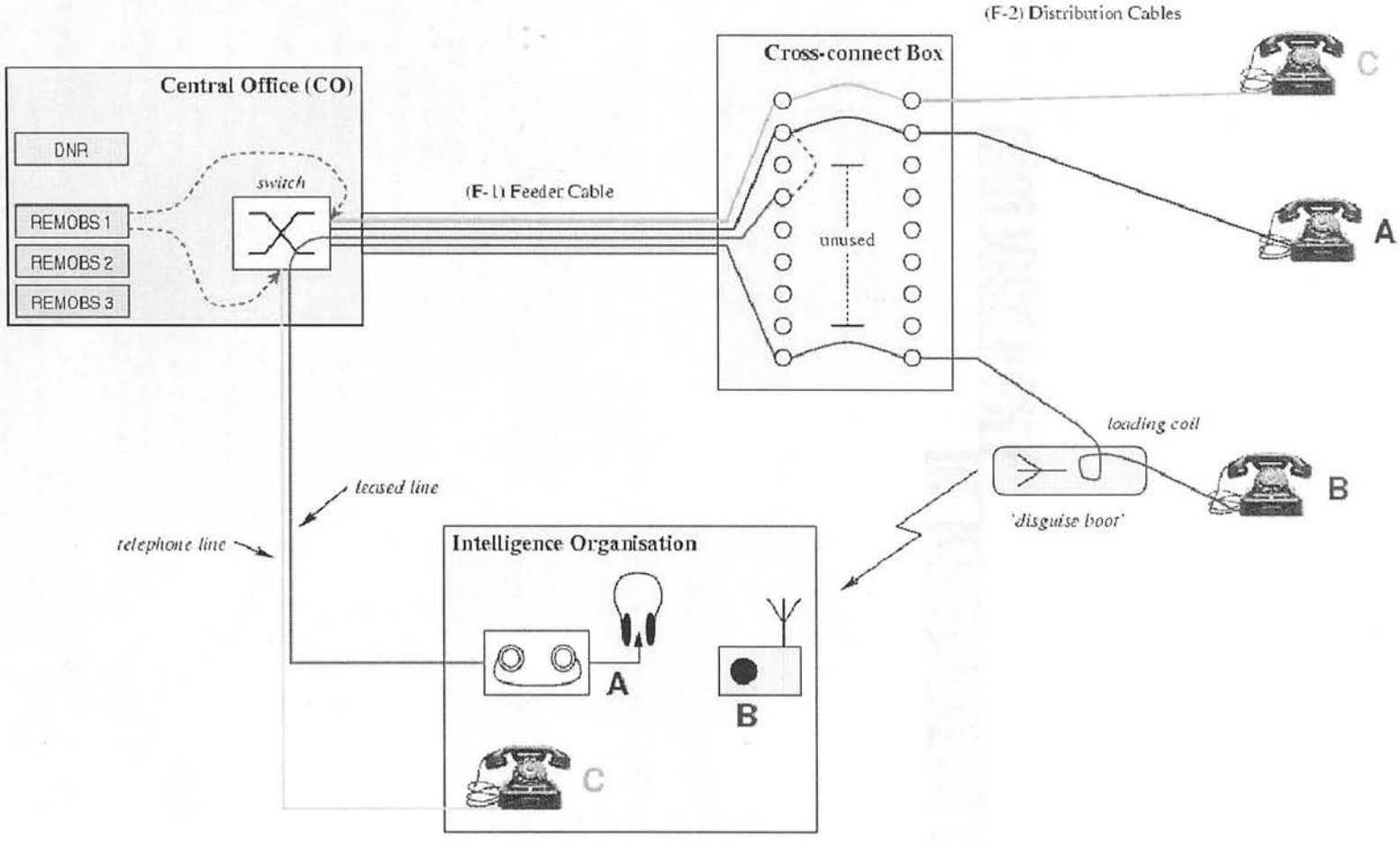


Diagram 6.1.2 The four distinct models of analogue CI are shown here. Connection A shows a hardwired tap installed at the cross-connect box; connection B shows a hardwired tap installed at the loading coil; and connection C shows a softwire tap conducted through a REMOBS unit. A communications data request is also shown by the DNR box inside the Central Office (CO) location.

BIBLIOGRAPHY OF REFERENCES CITED

Bibliography of References Cited.

Abramson, J.B. *et al.* (1988) *The Electronic Commonwealth: The Impact of New Technologies Upon Democratic Politics*, Basic Books, New York City, NY.

Ackroyd, C. *et al.* (1980) *The Technology of Political Control*, Penguin Books, Ltd., Harmondsworth, Middlesex.

Ackroyd, S. *et al.* (1992) *New Technology and Practical Police Work: The Social Context of Technical Innovation*, Open University Press, Buckingham.

Ahmed, K. (2000) "Secret Plan to Spy on All British Phone Calls", *The Observer*, London, 03 December 2000.

Akdeniz, Y. (2000) "New Privacy Concerns: ISPs, Crime Prevention and Consumers' Rights", *International Review of Law, Computers and Technology*, 14(1), pp55-61.

Akdeniz, Y. *et al.* (1999) *Who Watches the Watchmen Part III: ISP Capabilities for the Provision of Personal Information to the Police*, Cyber-Rights & Cyber Liberties UK, Leeds, February <http://www.cyber-rights.org/privacy/watchmen-iii.htm> last accessed 12 April 2001.

Akdeniz, Y. *et al.* (2001) "BigBrother.gov.uk: State Surveillance in the Age of Information and Rights", *Criminal Law Review*, February, pp73-90.

Akdeniz, Yaman, Director, *Cyber-Rights & Cyber-Liberties UK*, Interview to Joseph Fitsanakis, Leeds, England, Friday 05 May 2000 (recorded).

Almond, G.A. (1960) "A Functional Approach to Comparative Politics", in G.A. Almond & J.S. Coleman (eds.) *The Politics of the Developing Areas*, Princeton University Press, Princeton, NJ, pp94-128.

American Friends Service Commitee (1979) *The Police Threat to Political Liberty*, AFSC, Philadelphia, PA.

Anderson, R. *et al.* (1999) "Unprecedented Safeguards for Unprecedented Capabilities", paper presented at *Hoover Institution National Security Forum Conference* entitled *International Cooperation to Combat Cyber Attacks*, Stanford University, Stanford, CA, 07 December 1999 (copy on file with author).

Andrew, C. (1985) *Secret Service: The Making of the British Intelligence Community*, Heinemann, London.

Andrew. C. & O. Gordievsky (1990) *KGB: The Inside Story of Its Foreign Operations from Lenin to Gorbachev*, Harper Collins, New York City, NY.

Anon (1994) "British Telecom Security Contact Information", *2600 Magazine*, New York City, NY, June.

Anon (1996a) "FBI Pressed by Industry for Better Wiretap Data", *Communications Daily*, Washington DC, 18 January.

Anon (1996b) "Clinton Administration, Congress, Propose Sweeping Anti-Terrorism Initiatives", *CDT Policy Post*, 2(29), Washington, DC, 01 August.

Anon (1997a) *Industry and Privacy Advocates' Response to FBI CALEA Implementation Plan*, CTIA, USTA, PCIA, CDT, Washington, DC, 29 April, <http://www.cdt.org/digi_tele/970429_resp.html> last accessed 19 May 1999.

Anon (1997b) *Analysis of Emerging Technologies and Services*, 2nd ed., Booz Allen & Hamilton, Washington, DC, March (marked "for official use only", copy on file with author).

Anon (1998a) *FBI Tries to Use CALEA to Expand Its Surveillance Capabilities*, Centre for Democracy and Technology, Washington, DC, <http://www.cdt.org/digitele/expand.html>, last accessed 13 May 1999.

Anon (1998b) *Wiretap Overview: The Nature and Scope of Governmental Electronic Surveillance Activity*, Centre for Democracy and Technology, Washington, DC, 22 May.

Anon (1998c) *Big Brother in the Wires: Wiretapping in the Digital Age*, ACLU, Wye Mills, Maryland, March, <http://www.aclu.org/issues/cyber/wiretap_brother. html> last accessed 13 May 1999.

Anon (1998d) "FBI Claims Substantial Progress, Facts Show Otherwise", *CDT Policy Post*, 4(3.2), 18 February.

Anon (1999a) *Response to the Interception of Communications Consultation Paper*, ISPA, London, August <http://www.ispa.org.uk/html/august_1999.htm> last accessed 29 August 1999.

Anon (1999b) *Response to the Interception of Communications Act Consultation Exercise*, Scottish Telecom, Glasgow, 13 August (copy on file with author).

Anon (1999c) *CALEA: A Precedent for Domestic Encryption Controls?*, Centre for Democracy and Technology, Washington, DC.

Anon (1999d) *Interception of Communications in the United Kingdom*, Nortel Networks, London (copy on file with author).

Anon (1999e) *Alliance for Electronic Business Response to Interception of Communications in the UK*, Alliance for Electronic Business, London, August.

Anon (2000a) *STAND's Guide to the RIP v1.0*, STAND, London, 29 February, <http:// www.stand.org.uk/ripnotes> last accessed 08 April 2000.

Anon (2000b) *Wiretap Overview: The Nature and Scope of Governmental Electronic Surveillance Activity*, Centre for Democracy and Technology, Washington, DC, 08 May.

Anon (2001) *Head of National Technical Assistance Centre (NTAC) Announced*, Home Office News Release, London, 30 March 2001.

Appleby, C. (1995) "Making Security a Reality for All: Businesses count on effective computer encryption technologies to make electronic commerce and cellular communications safe for all users", *Information Week*, New York City, NY, 09 January 1995, <http://www.infoweek.com/509/08encry.htm> last accessed 22 November 1997.

Apter, D.E. (1965) *The Politics of Modernisation*, University of Chicago Press, Chicago, IL.

Aronson, S.H. (1977) "Bell's Electrical Toy: What's the Use? The Sociology of Early Telephone Usage" in I.de S. Pool (ed.) *The Impact of the Telephone*, MIT Press, Cambridge, Massachusetts, pp15-39.

Auble, D. & D. Bender (2000) "CALEA Capacity Requirements: What You Need To Know", presentation given at the *103rd Annual United States Telecommunications Association Convention and Exhibition*, Miami Beach, Florida, 02 October.

Aubrey, C. (1981) *Who is Watching You? Britain's Security Services and the Official Secrets Act*, Pelican Books, Middlesex.

Aubrey, C. (1998) "Of Course MI5 is Lying. That is its Job", *New Statesman & Society*, 07 August, p14.

Baker, S.A (1994) "Don't Worry Be Happy", *Wired Magazine*, San Francisco, CA, issue 2.06, June.

Baker, S.A. *et al.* (1998) *Comments of the Telecommunications Industry Association Before the Federal Communications Commission in the Matter of CALEA*, CC Docket No 97-213, Washington, DC, 08 May (draft version; copy on file with author).

Baleanu, V.G. (1995) *The Enemy Within: The Romanian Intelligence Service in Transition*, Royal Military Academy Conflict Studies Research Centre, Camberley, Surrey.
Ball, D. (1989a) "Soviet Signals Intelligence: Vehicular Systems and Operations", *Intelligence and National Security*, 4(1), January, pp29-44.
Ball, D. (1989b) *Soviet Signals Intelligence SIGIN77: Intercepting Satellite Communications*, Australian National University Strategic and Defence Studies Centre, Canberra.
Bamford, J. (1982) *The Puzzle Palace*, Houghton Mifflin, Boston.
Barber, B.R. (1984) *Strong Democracy: Participation Politics for a New Age*, University of California Press, Berkeley, CA.
Barber, B.R. (1988) "Pangloss, Pandora or Jefferson? Three Scenarios for the Future of Technology and Democracy", in R. Plant *et al.* (eds.) *Information Technology: The Public Issues*, Alden Press, Oxford, pp177-192.
Bar-Joseph, U. (1995) *Intelligence Intervention in the Politics of Democratic States: The United States, Israel and Britain*, Pennsylvania State University Press, Pittsburgh, PA.
Barlow, J.P. & **D.E. Denning** (1994) "Online Debate Over the Clipper Chip Scheme", *Time Online forum of America On Line*, 10 March.
Barlow, J.P. (1994) "Jackboots on the Infobahn", *Wired Magazine*, issue 2.04, San Francisco, February, <http://www.cpsr.org/cpsr/privacy/crypto/clipper/barlow_wired_2.04_clipper> last accessed 15 October 1997.
Barry, E.E. (1965) *Nationalisation in British Politics: The Historical Background*, Jonathan Cape, London.
Baxter, J. D. (1990) *State Security, Privacy and Information*, Harvester & Wheatsheaf, New York City, NY.
Beer, M. (1920) *A History of British Socialism*, vol. II, G. Bell & Sons, Ltd., London.
Bell, D. (1973) *The Coming of Post Industrial Society*, Basic Books, New York City, NY.
Berman, J. & **J.X. Dempsey** (1996) *Comments on CALEA Capacity Notice, 60 Fed. Reg. 53643*, letter addressed to David F. Worthley, Unit Chief, FBITILU, Washington, DC, 16 January (copy on file with author).
Bertrand Russell Peace Foundation (1972) *Subversion in Chile: A Case Study in US Corporate Intrigue in the Third World*, Spokesman Books, Nottingham.
Blacharski, D. (1998) *Network Security in a Mixed Environment*, IDG Books, New York City, New York.
Blair, P.D. ***et al.*** (1995) *Electronic Surveillance in a Digital Age*, US Congress Office of Technology Assessment, Government Printing Office, Washington, DC, July.
Blank, S. (1973) *Industry and Government in Britain: The Federation of British Industries in Politics, 1945-1965*, Saxon House, Farnborough, Hants.
Bleep, B. (1992) "BT's Fight Against Fraud", BT Today Magazine, London, June.
Bolling, G.H. (1983) *AT&T, Aftermath of Antitrust: Preserving Positive Command and Control*, National Defence University, Washington, DC.
Booz-Allen & **Hamilton** (1997) *Analysis of Emerging Technologies and Services*, report produced for the ESTSFBI, Chantilly, VA, March, (copy on file with author).
Booz-Allen & **Hamilton** (1999) *Information Assurance and Information Operations*, Booz-Allen & Hamilton Consultants, McLean, VA, 16 August, <http://www.bah.com/army/ia_io_national_strategy.html>, last accessed 11 September 2000.
Booz-Allen & **Hamilton** (undated) *T1 Technology and Service Market Study*, Booz-Allen &

Hamilton Consultants, Chantilly, VA, (copy on file with author).
Boucher, R. & D. Edwards (1994) *Telecommunications Carrier Assistance to the Government*, Report 103-827, 103rd Congress, 2nd Session, FBI, Washington, DC, 04 October.
Bourne, I. (2001) "Data Retention and Law Enforcement Requirements: How Can the Two be Reconciled?", presentation given at the *12th ISPA Legal Forum*, London, 05 July.
Bowden, C., (2000) Director, *Foundation for Information Policy Research*, Interview to Joseph Fitsanakis, London, England, Wednesday 12 April 2000 (recorded)..
Branch, T. (1976) "The Trial of the CIA", *New York Times Magazine*, 12 September, p126.
Breckinridge, S.C. (1986) *The CIA and the World Intelligence System*, Westview Press, Boulder, CO.
Brenton, M. (1964) *The Privacy Invaders*, Coward-McCann Inc., New York City, NY.
Briggs, A. (1961) *The History of Broadcasting in the United Kingdom*, vol. I, Oxford University Press, Oxford.
Brooke, S. (1991) "Atlantic Crossing? American Views of Capitalism and British Socialist Thought, 1932-1962", *Twentieth Century British History*, 2 (2), pp107-136.
Brown, D. (2001) *Big Brother to Test Tapping Capabilities*, Interactive Week, San Francisco, CA, 18 June.
Brown, I. *et al.* (eds.) (2000) *The Economic Impact of the Regulation of Investigatory Powers Bill*, British Chambers of Commerce, London, 18 August.
Bunyan, T. (1976) *The History and Practice of the Political Police in Britain*, Julian Friedmann Publishers, London 1976.
Burton, M. (1994) "Government Spying for Commercial Gain", *CIA Studies in Intelligence*, 37(5), Washington DC, pp17-23.
Caiden, G.E. (1977) *Police Revitalisation*, Lexington Books, Lexington, MA.
Campbell, D. (1999) *Interception Capabilities 2000: A Report to the Director General for Research of the European Parliament*, European Union, Office of Scientific and Technical Options Assessment, Strasbourg, April 1999.
Campbell, D. (ed.) (1981) *Big Brother is Listening: Phone Tappers and the Security State*, New Statesman, London.
Canes, M. (1966) *Telephones: Public or Private? A Comparative Study of the British and American Systems*, Institute of Economic Affairs, London.
Carr, J.G. (1998) *Law on Electronic Surveillance*, West Group, St Paul, MN, 2nd edition, release No 23.
Carroll, J.A. (1969) *The Third Listener*, E.P. Dutton & Co., Inc., New York City, NY.
Carter, A.B. (1989) "Telecommunications Policy and US National Security", in R.W. Crandall & Kenneth Flamm (eds.) *Changing the Rules: Technological Change, International Competition and Regulation in Communications*, The Brookings Institution, Washington, DC, pp221-256.
Carter, D. (1959) *The Fourth Branch of Government*, Houghton Mifflin, Boston, MA.
Castells, M. (1989) *The Informational City: Information Technology, Economic Restructuring, and the Urban-Regional Process*, Basil Blackwell, Oxford.
Challenor, T. (undated) Letter addressed to Benjamin Laurie, Internet Network Services Ltd., London, <http://www.cyber-rights.org/privacy/individu.htm> last accessed 13 December 2000.
Champion, M. (2000) "UK Internet Tapping Bill Stays Intact; Amended Text Addresses Privacy Issues", *The Wall Street Journal*, Princeton, NJ, 17 July <http://cryptome.org/rip-intact.htm> last accessed 18 July 2000.
Charlesworth, A. *et al.* (1996) *An Atlas of Industrial Protest in Britain, 1750-1990*,

Macmillan, Basingstoke, Hampshire.
Charney, S. & K. Alexander (1996) "Computer Crime", paper presented at the *Randolph W. Thrower Symposium: Legal Issues in Cyberspace: Hazards on the Information Superhighway*, 26-28 February, Atlanta, Georgia.
Chick, M. (1991) "Competition, Competitiveness and Nationalisation, 1945-1951", in G. Jones & M.W. Kirby (eds.) *Competitiveness and the State: Government and Business in Twentieth-Century Britain*, Manchester University Press, Manchester, pp60-77.
CIA (1953) *Relinquishing of Controls over Communications in Austria by the Soviets*, NN3-263-99-001, 18 November, RIP 06 May 1999.
CIA (1958) *Post and Telecommunications Services in the USSR, 1950-57*, NN3-263-98-002, 21 July, RNS 28 October 1997.
CIA (1962a) *Intra-Bloc and International Telecommunications of the Sino-Soviet Bloc*, NN3-263-00-001, 01 April, RIP 19 Nov 1999.
CIA (1962b) *Technology in Post and Telecommunications in the USSR*, NN3-263-98-002, 01 April, RNS 28 October 1997.
Cisneros, O.S. (2000) "These Wires Were Made for Tapping", *Wired News*, San Francisco, CA, 14 August, <http://www.wired.com/news/politics/0,1283,38170, 00.html> last accessed 14 August 2000.
Clark, J., *et al.* (1989) *The Process of Technological Change: New Technology and Social Choice in the Workplace*, Cambridge University Press, Cambridge.
Clayton R., *et al.* (2000) *Response to the Smith Group Report for the Home Office on Technical and Cost Issues Associated with Interception of the Internet*, ISPA, London, 23 May, <http://www.ispa.org.uk/html//updateable_smithreport.htm> last accessed 22 September 2000.
Clayton R., *et al.* (2000) *Response to the Smith Group Report for the Home Office on Technical and Cost Issues Associated with Interception of the Internet*, ISPA, London, 23 May, <http://www.ispa.org.uk/html//updateable_smithreport.htm> last accessed 22 September 2000.
Cohen, J.E. (1992) *The Politics of Telecommunications Regulation: The States and the Divestiture of AT&T*, M.E. Sharpe, Armonk, NY.
Cohen, S. & A. Scull (1985) "Social Control in History and Sociology", in S. Cohen & A. Scull (eds.) *Social Control and the State: Historical and Comparative Essays*, Basil Blackwell, Oxford, pp1-14.
Cohn, C. (2000) *CALEA Impact*, electronic message addressed to Joseph Fitsanakis, EFF, San Francisco, CA, 29 June (copy on file with author).
Cole, C. (1999a) *Internet Users Privacy Forum Minutes: Meeting One*, London Internet Exchange, Peterborough, 22 March.
Cole, C. (1999b) *Internet Users Privacy Forum Minutes: Meeting Two*, Easynet, London, 02 June.
Command 108 (1987) *Interception of Communications Act*, HMSO, London, March.
Command 108 (1987) *Interception of Communications Act*, HMSO, London, March.
Command 283 (1957) *Report of the Committee of Privy Councillors Appointed to Inquire into the Interception of Communications*, HMSO, London, September [often referred to as 'the report of the Birkett Commission'].
Command 283 (1957) *Report of the Committee of Privy Councillors Appointed to Inquire into the Interception of Communications*, HMSO, London, September [often referred

to as 'the report of the *Birkett Commission*'].
Command 4778 (2000) *Interception of Communications Act 1985: Report of the Commissioner for 1999*, HMSO, London, July.
Command 7873 (1980) *The Interception of Communications in Great Britain*, HMSO, London, April.
Command 7873 (1980) *The Interception of Communications in Great Britain*, HMSO, London, April.
Command 9843 (1985) *The Interception of Communications in Great Britain*, HMSO, London, February.
Command 9843 (1985) *The Interception of Communications in Great Britain*, HMSO, London, February.
Corn-Revere, R. (2000) *The Fourth Amendment and the Internet: Testimony Before the Subcommittee on the Constitution of the Committee on the Judiciary*, US House of Representatives, Washington, DC, 06 April.
Coryell, G. (2001) "Pentagon May Expand CIA's Domestic Role", *The Tampa Tribune*, 12 August 2001, <http://tampatrib.com/floridametronews/MGAMZCKCAQC. html> last accessed 12 August 2001.
Courtney, R. (2000) *CDT and CALEA*, electronic message addressed to Joseph Fitsanakis, CDT, Washington, DC, 03 July (copy on file with author).
Cruise-O'Brien, R. & G.K. Helleiner (1983) "The Political Economy of Information in a Changing International Economic Order", in R.C. Cruise-O'Brien (ed.) *Information, Economics and Power: The North-South Dimension*, Hodder & Stoughton, London, pp1-27.
Curry, J.C. (1999) *The Security Service 1908-1945: The Official History*, Public Record Office, Kew.
Cutright, P. (1963) "National Political Development: Measurement and Analysis", *American Sociological Review*, No 28, April, pp253-264.
Dandeker, C. (1990) *Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to the Present Day*, Polity Press, Cambridge.
Danelian, N.R. (1939) *AT&T: The Story of Industrial Conquest*, Vanguard Press, New York City, NY.
Dash, S., *et al.* (1959) *The Eavesdroppers*, Rutgers University Press, New Brunswick, NJ.
Davies, S. (1997) "Spies Like US", *The Daily Telegraph*, 16 December.
de Stempel, C. (2001) "AOL's monitoring costs", comments made at the *12th ISPA Legal Forum*, London, 05 July.
Dean, J.P. & W. Foote-Whyte (1970) "How Do You Know If the Informant Is Telling the Truth?", in L.A. Dexter *Elite and Specialised Interviewing*, Northwester University Press, Evanston, IL, pp119-131.
Delio, M. (2001) "ISPs 'RIP' Into British Police", *Wired News*, San Francisco, CA, 19 January, <http://www.wired.com/news/politics/0,1283,41288,00.html> last accessed 21 January 2001.
Demac, D.A. (1984) *Keeping America Uninformed: Government Secrecy in the 1980s*, Pilgrim Press, New York City, NY.
Dempsey, J.X. & A. Oram (1998) *Reply Comments Before the Federal Communications Commission Regarding the Implementation of CALEA*, CC Docket No 97-213, Washington, DC, 11 February.

Dempsey, J.X. (1995) *Memorandum on Capacity Requirements Under CALEA*, Centre for National Security Studies, Washington, DC, 09 November.
Dempsey, J.X. (1998) *Comments Before the Federal Communications Commission in the Matter of CALEA Extension of October 1998 Compliance Date*, CC Docket No 97-213, Centre for Democracy and Technology, Washington, DC, 02 April.
Dempsey, J.X. (1999) *FBI Seeks to Impose Surveillance Mandates on Telephone System; Balanced Objectives of 1994 Law Frustrated*, Centre for Democracy and Technology, Washington, DC, 04 March.
Denning, D.E. (1993) "To Tap or Not to Tap", *Communications of the ACM*, 36(3), pp377-383.
Denning, D.E. (1994) "Campaign and Petition Against Clipper", *Privacy Forum Digest*, 3(4), Woodland Hills, CA, 20 February, pp566-575.
Department of Trade and Industry (1996) *Development of the Information Society: An International Analysis*, HMSO, Norwich.
Depla, P.F.G. & P.W. Tops (1995) "Political Parties in the Digital Era: The Technology Challenge?", in W.B.H.J. van de Donk *et al.* (eds.) *Orwell in Athens: A Perspective on Informatisation and Democracy*, IOS Press, Amsterdam, pp155-178.
Deutsch, K.W. (1963) *The Nerves of Government: Models of Political Communication and Control* The Free Press, New York City, NY.
Dexter, L.A. (1970) *Elite and Specialised Interviewing*, Northwestern University Press, Evanston, IL.
Diffie, W. & S. Landau (1998) *Privacy on the Line: The Politics of Wiretapping and Encryption*, MIT Press, Cambridge, MA.
Dillon, J.T. (1990) *The Practice of Questioning*, Routledge, London.
Dillon, M. (1999) *The Dirty War: Covert Strategies and Tactics Used in Political Conflicts*, Routledge, New York City, NY.
Dilts, M.M. (1914) *The Telephone in a Changing World*, Longman's Green, New York City, NY.
Donner, , F.J. (1988) "The Emergence of Surveillance Societies in the Western World: Toward the Year 2000", *Government Information Quarterly*, 4(5), pp377-387.
Donner, F.J. (1980) *The Age of Surveillance: The Aims and Methods of America's Political Intelligence System*, Alfred A. Knopf, New York City, NY.
Dordick, H.S. & G. Wang (1993) *The Information Society: A Retrospective View*, Sage Publications, London.
Dorobek, C.J. (2001) "Bill Clamps Down on Carnivore", *Federal Computer Week*, Washington, DC, 25 July.
Dorsen, N. & S. Gillers (eds.) (1974) *None of Your Business: Government Secrecy in America*, Viking Press, New York City, NY.
Douglas, J.D. (1970) Freedom and Tyranny: Social Problems in a Technological Society, Alfred A. Knopf, New York City, NY.
Douglas, W.O. (1954) *An Almanac of Liberty*, Doubleday, Garden City, NY.
Economist Magazine (1995) *The Death of Distance Survey*, London, September.
EITC (1868) *Government and Telegraphs: Statement of the Case of the EITC Against the Government Bill for Acquiring the Telegraphs*, EITC, London.
Electronic Surveillance Task Force (1997) *Communications Privacy in the Digital Age: Interim Report*, Digital Privacy and Security Working Group, Washington, DC, June, <http://www.cdt.org/digi_tele/9706rpt.html> last accessed 19 May 1999.

Elliff, J.T. (1972) "The FBI and Domestic Intelligence", in R.H. Blum (ed.) *Surveillance and Espionage in a Free Society: A Report by the Planning Group on Intelligence and Security to the Policy Council of the Democratic National Committee*, Praeger Publishers, New York City, NY, pp20-45.

Ellul, J. (1965) *The Technological Society*, Johnathan Cape, London.

Ellul, J. (1989) *What I Believe*, Eerdmans, London.

Emery, D. (1999) *Consultation Response*, ICL, Slough, 10 August (copy on file with author).

Emsley, C. (1996) *The English Police: A Political and Social History*, Longman, London, 2nd edition.

Ericson, R.V. & K.D. Haggerty (1997) *Policing the Risk Society*, University of Toronto Press, Toronto.

Etzioni-Halevy, A. (1983) *Bureaucracy and Democracy: A Political Dilemma*, Routledge & Kegan Paul, London.

European Commission (1995) *G7 Ministerial Conference on the Global Information Society*, Office for Official Publications of the European Communities, Luxembourg.

Evans, C.A. (1972) "Proposals for Renovating the FBI" in R.H. Blum (ed.) *Surveillance and Espionage in a Free Society: A Report by the Planning Group on Intelligence and Security to the Policy Council of the Democratic National Committee*, Praeger Publishers, New York City, NY, pp46-52.

Evans, V. (1999) *Internet Users Privacy Forum Minutes: Meeting Three*, Easynet, London, 02 September.

Feldman, J. (2000) "Digital Sculduggery: Online Sleuths Tell All", transcript of Interview with Dana Hawkins, *US News and World Report*, 02 October 2000, <http://www.usnews.com/usnews/issue/001002/nycu/privacy.b.htm> last accessed 14 October 2000.

Fisk, J. (1996) *Media Matters*, University of Minnesota Press, London.

Fitzgerald, P. & M. Leopold (1987) *Stranger on the Line: The Secret History of Phone Tapping*, The Bodley Head, London.

Fitzgerald, P. (1994) "All About Eavesdropping", *The New Statesman & Society*, London, 29 July, pp30-31.

Flaherty, D. (1989) *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States*, University of North Carolina Press, Raleigh, NC.

Foucault, M. (1977) *Discipline and Punish: The Birth of the Prison*, Pantheon Books, New York City, NY.

Foucault, M. (1983) "Power, Sovereignty and Discipline", in D. Held, *et al.* (eds.) *States and Societies*, Martin Robertson, Oxford, pp296-312.

Freeh, L. (1995) Letter addressed to Henry Hyde, Chairman of the US House of Representatives Committee on the Judiciary, FBI, Chantilly, VA, 02 November, <http://www.cdt.org/policy/digtel/freeh_hyde_ltr.html> last accessed 01 December 1997.

Freeh, L. (1997a) *Statement Before the US Senate Committee on Appropriations Hearing on Counter-Terrorism*, S. Hrg. 46-491, 105th Congress, 1st Session, US Government Printing Office, Washington DC, 13 May.

Freeh, L. (1997b) *Excerpts from Testimony to the Senate Judiciary Committee*, Centre for Democracy and Technology, Washington, DC, 04 June, <http://www.ctd.

org/digi_tele/970604_Freeh.html> last accessed 14 June 1997.
Freeh, L. (2000) *Statement Before the Subcommittee on Technology, Terrorism and Government Information of the US Senate Committee on the Judiciary on Examining the Incidence of Cyber Attacks on the Nation's Information Systems: Removing Roadblocks to Investigation and Information Sharing*, S. Hrg. 106-839, 106th Congress, 2nd Session, Government Printing Office, Washington, DC, 28 March.
Frey, F.W. (1973) "Communication and Development", in I. de S. Pool & W. Schramm (eds.) *Handbook of Communication*, Rand McNally, Chicago, IL, pp337-461.
Friedman, L. (1973) *A History of American Law*, Simon & Schuster, New York City, NY.
Frost, M. (1994) *Spyworld: Inside the Canadian and American Intelligence Establishments* (as told to M. Gratton), Doubleday Canada, Toronto.
Frost, M. (1996) "Second Thoughts from the Second Oldest Profession: Inside the US-Canada Spyworld", *Covert Action Quarterly*, No. 59, Washington, DC.
Fuld, L. (1909) *Police Administration*, Patterson Smith, New York City, NY.
Galbraith, J.K. (1967) *The New Industrial State*, Houghton Mifflin Co., Boston, MA.
Gandy Jr, O.H. (1989) "The Surveillance Society: Information Technology and Bureaucratic Social Control", in M. Siefert, G. Gerbner & J. Fisher (eds.) *The Information Gap: How Computers and Other New Communication Technologies Affect the Social Distribution of Power*, Oxford University Press, Oxford, pp61-76.
Gandy Jr, O.H. (1993) *The Panoptic Sort: A Political Economy of Personal Information*, Westview Press, Boulder, Co.
Garnet, R.W. (1985) *The Telephone Enterprise: The Evolution of the Bell System's Horizontal Structure, 1876-1909*, Johns Hopkins University Press, Baltimore, MD.
Gaspar, R. (2000) *Looking to the Future: Clarity of Communications Data Retention Law*, NCIS Submission on Communications Data Retention Law, NCIS, London 21 August (copy on file with author).
Giddens, A. (1985) *The Nation State and Violence: A Contemporary Critique of Historical Materialism*, Polity Press, Cambridge.
Gill, P. (1994) *Policing Politics: Security Intelligence and the Liberal Democratic State*, Frank Cass, London.
Gilpin, R. (1975) *US Power and the Multinational Corporation*, Basic Books, New York City, NY.
Godson, R. (1996) *Dirty Tricks or Trump Cards: US Covert Action and Counterintelligence*, Brassey's Inc., Washington, DC, 1995.
Goralski, W.J. & **M. Kolon** (2000) *IP Telephony*, McGraw-Hill, San Francisco, CA.
Grey, D.L. (1999) *Consultation Paper on the Interception of Communications In the United Kingdom*, letter addressed to the Home Office's Interception Legislation Team, Durham Police Constabulary, Durham, 15 July (copy on file with author).
Hall, C. ***et al.*** (1999) *Response to the Interception of Communications Act Consultation Exercise*, Demon Internet, London, 19 August (copy on file with author).
Halperin, M.H. ***et al.*** (1977) *The Lawless State: The Crimes of the US Intelligence Agencies*, Penguin Books, Ltd., Harmondsworth, Middlesex.
Harden, I. & **N. Lewis** (1988) *The Noble Lie: The British Constitution and the Rule of Law*, Hutchinson, London.
HCSCF (2000) *Regulation of Investigatory Powers Bill*: *First Sitting*, Report of Proceedings, London, 14 March.
HCSCTI (2000) *Second Special Report: The Draft Electronic Communications Bill*, HMSO, London, 19 January.

HCTISC (1999a) *Seventh Report: Building Confidence in Electronic Commerce*, HC 187, HMSO, London, 19 May.
HCTISC (1999b) *Fourteenth Report: Draft Electronic Communications Bill*, HC 862, HMSO, London, November.
HCTISC (2000) *Third Special Report: Further Government Observations on the Fourteenth Report from the Trade and Industry Committee on the Draft Electronic Communications Bill*, HC 199, HMSO, London, February.
Headrick, D.R. (1991) *The Invisible Weapon: Telecommunications and International Politics, 1851-1945*, Oxford University Press, New York.
Heap, N. *et al.* (1995) *Information Technology and Society: A Reader*, Sage Publications & Open University Press, London.
Heupel, R. (1999) "CommNet Cellular Signs US$35 Million Deal with Nortel Networks For Network Modernization Software Upgrades", *Nortel Networks News Release*, Brampton, Ontario, 19 January, <http://www.notelnetworks.com/ corporate/ news/newsreleases/1999a/1_19_9999016_CommNet.html> last accessed 28 January 1999.
Hildebrand, T.A. (2000) "This Month in CALEA", *This Month In CALEA*, FBI, Chantilly, VA (copy on file with author).
Hildebrand, T.A. (2000) "TMIC Notes", *This Month in CALEA*, FBI, CIS, Raleigh, NC, 14 November.
Hills, J. (1986) *Deregulating Telecoms: Competition and Control in the United States, Japan and Britain*, Frances Pinter, London.
Hinton, J. (1983) *Labour and Socialism: A History of the British Labour Movement, 1867-1974*, Wheatsheaf Books, Brighton, Essex.
Holland, J.J. (2001) "Senate OKs Expanding Wiretap Law", Associated Press, New York City, New York, 13 September, <http://us.news2.yimg.com/f/42/31/7m/ dailynews.yahoo.com/h/ap/20010913/us/attacks_wiretapping_1.html>, last accessed 13 September 2001.
Hollander, R. (1985) *Video Democracy: The Vote-from-Home Revolution*, Lomond Press, Mount Airy, MD.
Holleran, J. (1999) *Comments on the Consultation Paper Issued by the Home Secretary on the 23 June in Respect to the Proposals for the Interception of Communications in the United Kingdom*, TUFF press statement, London (copy on file with author).
Holton, R. & **Turner, B.** (1989) *Max Weber on Economy and Society*, Routledge, New York City, NY.
Home Office (1977) *Consolidated Circular to the Police on Crime and Kindred Matters*, HMSO, London.
Home Office (2001a) Regulation of Investigatory Powers Act 2000: Consultation on the Section 13 Order, London, 09 March, <http://www.homeoffice.gov.uk/ripa/con sec13.htm> last accessed 13 April 2001.
Home Office (2001b) *Consultation on Section 12 of the Regulation of Investigatory Powers Act 2000*, London, 29 June, <http://www.homeoffice.gov.uk/ripa/section 12.htm> last accessed 01 July 2001.
Home Office (2001c) *National Technical Assistance Centre*, London 15 August, <http: //www.homeoffice.gov.uk/oicd/ecu/ntac.htm> last accessed 17 August 2001.
Horner, M. (1996) *Information, Technology and the Information Society*, The British Library, London.
House of Commons (2000) *Regulation of Investigatory Powers Bill*, Hansard vol. 345, cols

776-837, 02 November.
Hughes, P. (1981) *British Broadcasting: Programmes and Power*, Chartwell-Bratt, Bromley, Kent.
Hunt, E.H. (1981) *British Labour History, 1815-1914*, Weidenfeld & Nicolson, London.
Int02. Communications Intelligence Officer (former), *Special Branch*, London, England, 12 April 2000 (recorded).
Int03. External Maintenance Engineer, Engineering Division (former, currently a Consultant for Internet service provider firm), *British Telecom, Plc*, Bristol, England (recorded).
Int04. Fraud Control and Revenue Assurance Manager, *Energis Communications, Ltd*, Reading, England, 09 May 2000 (recorded).
Int06. Fraud Control Manager, *GTS Telecommunications, Ltd*, Reading, England, Friday 12 May 2000 (recorded).
Int07. Security Officer, *British Telecom, Plc*, London, England, 08 May 2000 (recorded).
Int08. Chief Executive Officer, *Colloquium Internet, Ltd*, Paisley, Scotland, Friday 28 April 2000 (recorded).
Int09. Fraud Liaison Officer, *One Tel, Plc*, London, England, Wednesday 03 May 2000 (recorded, Greek language, translated by the author).
Int10. Regulation Officer, *London Internet Exchange, Ltd*, Peterborough, England, Wednesday 10 May 2000 (recorded).
Int11. Regulatory Affairs Officer, *British Telecom, Plc*, London, England, Wednesday 12 April 2000 (recorded).
Int12. Chief Executive Officer, *The Telecommunications United Kingdom Fraud Forum, Federation of Communications Services*, London, England, Tuesday 11 April 2000 (recorded).
Int13. Technical Unit Chief, Emergency Communications Unit, *organisation withheld for privacy reasons*, Bluff City, Tennessee, Saturday 23 December 2000 (recorded).
Int14. Sergeant, First Class, Communications Officer (on inactive duty), *United States Special Forces*, Franklin, Tennessee, Wednesday 12 January 2000 (recorded).
Int15. Sergeant, First Class, Communications Officer (on inactive duty), *United States Special Forces*, Franklin, Tennessee, Friday 02 June 2000 (recorded).
Int16. Director, National Services Planning, *United States Telecommunications Association*, Miami Beach, Florida, Tuesday 03 October 2000 (recorded).
Int17. Technical Director, *Organisation for the Promotion and Advancement of Smaller Telecommunications Companies*, Miami Beach, Florida, Monday 02 October 2000 (recorded).
Int18. Director, Government Relations, *Organisation for the Promotion and Advancement of Smaller Telecommunications Companies*, Miami Beach, Florida, Monday 02 October 2000 (recorded).
Int19. Unit Chief, Telecommunications Industry Liaison Unit, CALEA Implementation Section, *Federal Bureau of Investigation*, Atlanta, Georgia, Wednesday 15 November 2000 (recorded).
Int20. CALEA Compliance Attorney, *BellSouth USA*, Atlanta, Georgia, Friday 15 June 2001 (recorded).
Int21. CALEA Project Manager, *BellSouth, USA*, Atlanta, Georgia, Friday 15 June 2001 (recorded).
ISPA (1998) *Industry Capabilities for the Provision of Information*, ISPA, London,

February.
Jayko, M. (ed.) (1988) *FBI on Trial: The Victory in the Socialist Workers Party Suit Against Government Spying*, Pathfinder Press, New York City, NY.
Jeffery, K. & **P. Hennessy** (1983) *States of Emergency: British Governments and Strikebreaking Since 1919*, Routledge & Kegan Paul, London.
Jeffreys, D. (1995) *The Bureau: Inside the Modern FBI*, Houghton Mifflin Company, New York City, NY.
Jepperson, R.L. ***et al.*** (1996) "Norms, Identity and Culture in National Security", in P.J. Katzenstein (ed.) *The Culture of National Security: Norms and Identity in World Politics*, Columbia University Press, New York City, NY, pp33-74.
Johnson, L. (1988) *A Season of Inquiry: Congress and Intelligence*, Dorsey Press, Chicago, IL.
Jonquieres, G. de (1989) "The Deadly Mirage of Convergent Technology", The Financial Times, London, 24 July.
Joy, D. & **R.O. Wright** (1974) "Wiretaps in Perspective", in R.O. Right (ed.) *Whose FBI?*, Open Court, La Salle, IL, pp251-265.
Judge, J.F. (1985) "The Defence Communications Agency: Coping with Changing Times", *Defence Electronics*, vol. XVII, May, pp230-236.
Kahn, D. (1967) *The Codebreakers: The Story of Secret Writing*, MacMillan Publishing Co., New York City, NY.
Kallstrom, J.K. (1997) *Statement of FBI Assistant Director James K. Kallstrom Concerning the Second Notice of Capacity*, FBI National Press Office, Washington, DC, 14 January.
Kampschoer, G. (2000) "RIP Law is the Least of It", *Professional Security Magazine*, Wolverhampton, 11 October.
Kerr, D.M. (2000) *Statement of the FBI Laboratory Division Before the USCJ: Carnivore Diagnostic Tool*, Washington, DC, 06 September.
Kessler, R. (1993) *The FBI: Inside the World's Most Powerful Law-Enforcement Agency*, Pocket Books, New York City, NY.
Kieve, J. (1973) *The Electric Telegraph: A Social and Economic History*, David & Charles, Newton Abbot.
King, A. (1984) *The Coming Information Society*, The British Library, London.
Kirk, N. (1994) *Labour and Society in Britain and the USA: Challenge and Accommodation, 1850-1939*, vol. II, Scolar Press, Aldershot, Hants.
Klerks, P. (1995) "Covert Policing in the Netherlands" in C. Fijnaut & G.T. Marx (eds.) *Undercover: Police Surveillance in Comparative Perspective*, Kluwer Law International, The Hague, pp103-140.
Knight, A. (1990) *The KGB: Police and Politics in the Soviet Union*, Unwin Hyman, Boston, MA.
Kramer, M. (2000) "CIA Releases Largest-Ever Batch of Declassified Documents", Cable News Network, Atlanta, GA, 02 October, <http://www.cnn.com/2000/US/10/02/cia.documents/index.html>, last accessed 20 November 2000.
Krasner, S.D (1978) *Defending the National Interest: Raw Materials Investments and US Foreign Policy*, Princeton University Press, Princeton, NJ.
Lambert, J.L. (1986) *Police Powers and Accountability*, Croom Helm, London.
Lansman, N. (2000) Letter addressed to Charles Clarke, MP, Minister of State, ISPA, London, 31 May, <http://www.ispa.org.uk/html//updateable_ccletter.htm> last

accessed 01 September 2000.
Lapidus, E.J. (1974) *Eavesdropping on Trial*, Hayden Book Company, Inc., Rochelle Park, NJ.
Larsen, T. (1997) *Bench-Tested Circuits for Surveillance and Countersurveillance Technicians*, Paladin Press, Boulder, CO.
Leahy, P. (1995) Letter addressed to Louis Freeh, Director of the FBI, United States Congress, Washington, DC, 03 November, <http://www.cdt.org/policy/digtel/leahy_freeh_ltr.html> last accessed 01 December 1997.
Leahy, P. (1999) *Statement Before the US Senate Committee on the Judiciary, Subcommittee on Criminal Justice Oversight During Hearing on the Responsibilities and Activities of the Criminal Division of the Department of Justice*, S. Hrg. 106-725, 106th Congress, 1st Session, US Government Printing Office, Washington DC, 17 July.
Lefort, C. (1986) *The Political Forms of Modern Society: Bureaucracy, Democracy, Totalitarianism*, Polity Press, Cambridge.
Leigh, D. (1980) *The Frontiers of Secrecy: Closed Government in Britain*, Junction Books, London.
Leigh, D. (1988) The Wilson Plot: *The Intelligence Services and the Discrediting of a Prime Minister*, 1945-1976, Heinemann, London.
Leigh, I. & L. Lustgarten (1989) "The Security Service Act 1989", *Modern Law Review*, 52(11), pp814-9.
Leigh, L.H. (1975) *Police Powers in England and Wales*, Butterworth, London.
LeMond, A. & R. Fry (1975) *No Place to Hide: A Guide to Bugs, Wire Taps, Surveillance and other Privacy Invasions*, St Martin's Press, New York City, NY.
Lemos, R. (2000) "FBI Releases First Carnivore Data", *ZDNet News*, San Francisco, CA, 04 October, <http://news.zdnet.co.uk/zdnetuk/news/story/0,s2081770,00. html> last accessed 05 July 2001.
Lemos, R. (2001) "FBI Taps in Hunt for Attackers", ZDNet News, San Francisco, CA, 12 September, <http://dailynews.yahoo.com/h/zd/20010912/tc/fbi_taps_isps_in_hunt_for_attackers_1.html> last accessed 12 September 2001.
Leonard, V.A. (1938) *Police Communication Systems*, University of California Press, Berkeley, CA.
Leonard, V.A. (1964) *Police Organisation and Management*, The Foundation Press, Brooklyn, New York, 2nd edition.
Lethin, R. (1995) "Talk by Admiral Bobby Inman at MIT", *Computer Professionals for Social Responsibility*, Washington DC, February, <http://www.cpsr.org/cpsr/lists/rre/Bobby_Inman_on_Clipper_and_ the> last accessed 11 September 1999.
LIAFIC (1980) *Secrecy or the Right to Know? A Study of the Feasibility of Freedom of Information for the United Kingdom*, LIAFIC, London.
Lipset, S.M. (1959) "Some Social Requisites of Democracy: Economic Development and Political Legitimacy", *American Political Science Review*, No 53, March, pp69-105.
Lloyd, C. (1993) "Spymasters Order Redesign of 'Too Secure' Mobile Phones", *The Sunday London Times*, 31 January.
Lustgarten, L. & I. Leigh (1994) *In from the Cold: National Security and Parliamentary Democracy*, Clarendon Press, Oxford.
Lowenthal, M. (1950) *The Federal Bureau of Investigation*, William Sloane Associates, New York City, NY.

Lowenthal, M. (2000) *Intelligence: From Secrets to Policy*, Congressional Quarterly Press, Inc., Washington, DC.
Lyon, D. (1994) *The Electronic Eye: The Rise of Surveillance Society*, Polity Press, Cambridge.
Maddison, P.F. (1999) Letter addressed to the Home Office's Organised and International Crime Directorate, Hertfordshire Constabulary, Welwyn Garden City, 23 July (copy on file with author).
Maddison, P.F. (2000) Letter addressed to Joseph Fitsanakis, Hertfordshire Constabulary, Welwyn Garden City, Hertfordshire, 27 March (on file with author).
Maguire, J.M. (1959) *Evidence of Guilt: Restrictions Upon its Discovery or Compulsory Disclosure*, Little, Brown & Company, Boston, MA.
Mahl, T.E. (1998) *Desperate Deception: British Covert Operations in the United States, 1939-1944*, Brassey's, Washington DC.
Mahler, J.M. (undated) *Comments Before the National Telecommunications and Information Administration of the Computer and Communications Industry Association in the Matter of Section 1201(g) of the Digital Millennium Copyright Act*, CC Docket No 990428110-9110-01, Washington, DC (copy on file with author).
Mansell, R. (1993) *The New Telecommunications: A Political Economy of Network Evolution*, Sage Publications, London.
Manwaring-White, S. (1983) *The Policing Revolution: Police Technology, Democracy and Liberty in Britain*, The Harvester Press, Sussex.
Martin, M. (1991) *"Hello, Central?": Gender, Technology and Culture in the Formation of Telephone Systems*, McGill-Queen's University Press, Montreal.
Marvin, C. (1988) *When Old Technologies Were New: Thinking About Electric Communication in the Late Nineteenth Century*, Oxford University Press, New York City, NY.
Marx, K. & Engels, F. (1977) *The German Ideology*, Laurence & Wishart, London [originally produced in 1845-1846].
Masuda, Y. (1981) *The Information Society as Post-Industrial Society*, Institute for the Information Society, Tokyo.
Mavor, J. (1916) *Government Telephones: The Experience of Manitoba, Canada*, Moffat, Yard & Co., New York City, NY.
McCullagh, D. (1998) "Shadow Cryptocrats", *CyberWire Dispatch*, Washington, DC, 04 February, <http://www.cyberwerks.com/cyberwire/cwd/cwd.98.02.25.html> last accessed 04 February 1998.
McCullagh, D. (2001) "Anti-Attack Feds Push Carnivore", *Wired News*, San Francisco, CA, 12 September, <http://www.wired.com/news/politics/0,1283,46747,00. html> last accessed 12 September 2001.
McHugh, J. & B. Cordwell (2000) "Carriers Must Comply With CALEA by May 2", *The OPASTCO Advocate*, Washington, DC, February, pp5-6.
McLure, J. (1984) *Cop World: Policing the Streets of San Diego*, Macmillan, London and Basingstoke.
Meeks, B.N. (1994) "The End of Privacy", *Wired Magazine*, issue 2.04, April.
Meeks, B.N. (2000) "Carnivore: The Truth is Worse Than You Thought", *ZDNet News*, San Francisco, CA, 18 October, <http://news.zdnet.co.uk/story/0,,t269s2082045, 00.html> last accessed 18 October 2000.
Melton, H.K. (1993) *CIA Special Weapons and Equipment: Spy Devices of the Cold War*,

Sterling Publishing, New York City, NY.
Meynard, J. (1968) Technocracy, Faber & Faber, London.
Miceli, J. (1998) *USTA and Other Carrier Organisations File Petition with FCC to Resolve Wiretap Issues*, USTA press statement, Washington, DC, 09 April, <http://www.cdt.org/rls98-21.html> last accessed 19 May 1999.
Michael, J. (1979) *The Politics of Secrecy: The Case for A Freedom of Information Law*, National Council for Civil Liberties, London.
Michels, R. (1915) *Political Parties: A Sociological Study of the Oligarchical Tendencies of Modern Democracy*, Jarrold & Sons, London.
Middlemas, K. (1986) *Power, Competition and the State. Volume I: Britain in Search of Balance, 1940-1961*, Macmillan, London.
Milano, J.V. (1995) *Soldiers, Spies and the Rat Line: America's Undeclared War Against the Soviets*, Brassey's Inc., Washington, DC.
Miles, I. (1988) *Information Technology and Information Society: Options for the Future*, PICT Policy Research Paper, University of Sussex, Sussex.
Mills, E. (1998) "Privacy Advocates Snub 'Operation-Action' Encryption Plan", *The Industry Standard*, San Francisco, CA, 15 July <http://thestandard.net.articles/article_ print/1,1454,1094,00.html> last accessed 07 October 1999.
Minnick, W. (1995) "China Under Cover", *Far Eastern Economic Review*, 02 March, p 38.
Molina, A.H. (1990) *The Development of Public Switching: Systems in the UK and Sweden*, Edinburgh PICT Working Paper No.19, Edinburgh.
Morgan, J. (1987) *Conflict and Order: The Police and Labour Disputes in England and Wales, 1900-1939*, Clarendon Press, Oxford.
Morris, C.G. (1998) *Reply Comments of the FBI Before the Federal Communications Commission Regarding the Implementation of CALEA*, CC Docket No 97-213, Washington, DC, 11 February.
Morris, C.G. (1999) *Comments Before the Federal Communications Commission in the Matter of CALEA*, CC Docket No 97-213, Washington DC, 13 May.
Mosca, G. (1939) *The Ruling Class*, McGraw-Hill Book Co., Inc., New York City, NY [originally produced in 1895].
Mosquera, M. (1998a) "Encryption Plan Lets United States Compete", *Techweb*, Manhasset, NY, 13 July, <http://www.techweb.com/wire/story/TWB19980713 S0014> last accessed 13 July 1998.
Mouzelis, N.P. (1967) *Organization and Bureaucracy: An Analysis of Modern Theories*, Routledge & Kegan Paul, London.
Munting, R. (1996) *An Economic and Social History of Gambling in Britain and the USA*, Manchester University Press, Manchester.
Murphy, D.E., *et al.* (1997) *Battleground Berlin: CIA vs. KGB in the Cold War*, Yale University Press, New Haven, CT.
Murphy, W.F. (1965) *Wiretapping on Trial: A Case Study in Judicial Process*, Random House, New York City, NY.
Murray, Sir E. (1927) *The Post Office*, G.P. Putnam's & Sons, Ltd, London.
Navasky, V. & **N. Lewin** (1973) "Electronic Surveillance" in P. Watters & S. Gillers (eds.) *Investigating the FBI*, Doubleday Co., Inc., Garden City, NY, pp297-337.
Negroponte, N. (1995) *Being Digital*, Hodder & Stoughton, London.
NIJ (2000) *NIJ Standard-0227.00, Digital Intercept System (DIS) for Integrated Services Digital Networks (ISDN)*, NIST, Gaithersburg, MD (FOUO).

Nojeim, G.T. (1996) *Proposed Expansion of Wiretapping in the Senate Immigration Bill S. 1394*, ACLU, Washington, DC, 24 February, <http://www.aclu.org/congress/s 1394.html> last accessed 13 May 1999.

Nojeim, G.T. (1999) *Memorandum on International Electronic Surveillance*, American Civil Liberties Union, Washington DC, 07 June 1999.

Nojeim, G.T. *et al.* (1998) Letter addressed to US Senators and Representatives, ACLU, Washington, DC, 12 February, <http://www.aclu.org/congress/lg021298a.html> last accessed 13 May 1999.

Nora, S. & Minc, A. (1978) *L' Informatisation de la Societe: Un Réport du Président de la France*, La Documentation Francaise, Paris.

Norton-Taylor, R. (1990) *In Defence of the Realm?*, Civil Liberties Trust, London.

Norton-Taylor, R. (1997) "Rank and File Caught in MI5's Cold War Paranoia", *The Guardian*, London, 26 August.

O'Doud, D. (1999) *Consultation Paper on the Interception of Communications in the United Kingdom: HMIC Observations on the Proposed Legislation*, HMIC, London, August (copy on file with author).

Olin-Wright, E. (1978) *Class, Crisis and the State*, New Left Books, London.

Olmsted, K.S. (1996) *Challenging the Secret Government: The Post-Watergate Investigations of the CIA and FBI*, The University of North Carolina Press, Chapel Hill, NC, 2nd ed.

Overstreet, H. & B. Overstreet (1969) *The FBI in Our Open Society*, W.W. Norton & Company, New York City, NY.

Parish, A.F.W. (1999) *Interception of Communications in the United Kingdom: A Consultation Paper*, letter addressed to the Home Office's Organised and International Crime Directorate, Federation of the Electronics Industry, London, 13 August (copy on file with author).

Parker, E.B. (1973) "Technological Change and the Mass Media", in I. de S. Pool & W. Schramm (eds.) *Handbook of Communication*, Rand McNally, Chicago, IL, pp619-645.

Parkhill, D. (1979) "The Necessary Structure", in D. Godfrey & D. Parkhill (eds.) *Gutenberg Two*, Press Porcepic, Toronto.

Parr, M. (1999) *SAQ Response to Interception of Communications*, electronic message addressed to the Home Office's Interception of Communications Legislation Team, SAQ Internet, Ltd., London, 13 August (copy on file with author).

Paul, B. (1953) "Interview Techniques and Field Relationships" in A.L. Kroeber (ed.) *Anthropology Today*, University of Chicago Press, Chicago, IL, pp430-451.

Pearson, T. (1998) *A Response from ISPA and ACPO/ISP/Government Forum*, letter addressed to Yaman Akdeniz, Cyber Rights & Cyber Liberties, UK, ISPA, London, 02 December, <http://www.cyber-rights.org/privacy/response.htm> last accessed 12 May 2001.

Perez-Diaz, V.M. (1978) *State, Bureaucracy and Civil Society: A Critical Discussion of the Political Theory of Karl Marx*, Macmillan, Basingstoke.

Perry, C.R. (1977) "The British Experience 1876-1912: The Impact of the Telephone During the Years of Delay", in I. de S. Pool (ed.) "The Impact of the Telephone", MIT Press, Cambridge, MA, pp69-96.

Perry, C.R. (1992) *The Victorian Post Office: The Growth of a Bureaucracy*, The Boydell Press/The Royal Historical Society, Woodbridge, Sufolk.

Perry, R. (1999) *Response to Questionnaire for Providers of Communications Services*, London Internet Exchange, Peterborough, 13 August (copy on file with author).

Perry, R. (2000a) *ICF Participating Member Organisations and Personnel*, ICF, Winchester, October, <http://www.internetcrimeforum.org.uk /members.html> last accessed 14 March 2001.
Perry, R. (2000b) *ICF Terms of Reference*, ICF, Winchester, <http://www.internetcrime forum.org.uk/homepage.html> last accessed 14 March 2001.
Perry, R. (2001) *Combating Computer Related Crime*, London Internet Exchange, Ltd., 02 March, <http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/Public Hearing Presentations/RolandPerryLINX.html> last accessed 05 July 2001.
Perry, R. (undated) "Internet Users Privacy Forum Attendance List", *London Internet Exchange, Ltd.*, Peterborough, <http://www.iupf.org.uk/m1attend.html> last accessed 05 July 2001.
Pertrow, S. (1994) *Policing Morals: The Metropolitan Police and the Home Office, 1870-1914*, Clarendon Press, Oxford.
Peters, B.G. (1984) *The Politics of Bureaucracy*, Longman, New York City, NY, 2nd edition.
Pfaltzgraff, R.L. (1984) "National Security Decision Making: Policy Implications", in R.L. Pfaltzgraff & U. Ra'anan (eds.) *National Security Policy: The Decision Making Process*, Archon Books, Guilford, CT, pp291-304.
Philips, D. & R.D. Storch (1994) "Whigs and Coppers: The Grey Ministry's National Police Scheme, 1832", *Historical Research*, No 67, p77-80.
Pierce, J.R. (1977) "The Telephone and Society in the Past 100 Years", in I. de S. Pool (ed.) *The Impact of the Telephone*, MIT Press, Cambridge, MA, pp159-195.
Plate, T. & A. Darvi (1981) *Secret Police: The Inside Story of a Network of Terror*, Doubleday & Company Inc., Garden City, NY.
Pollock, D.A. (1973) *Methods of Electronic Audio Surveillance*, Thomas Publishers, Springfield, IL.
Pool, I. de S. (1959) "Television: A New Dimension in Politics", in E. Bordick & A.J. Brodbeck (eds.) *American Voting Behaviour*, The Free Press, Glencoe, IL, pp236-261.
Pool, I. de S. *et al.* (1977) "Foresight and Hindsight: The Case of the Telephone", in I. de S. Pool (ed.) *The Impact of the Telephone*, MIT Press, Cambridge, MA, pp127-157.
Porat, M.U. (1978) "Global Implication of the Information Society", *Journal of Communication*, No44, winter.
Porter, B. (1987) *The Origins of the Vigilant State: The London Metropolitan Police Special Branch Before the First World War*, Weidenfeld & Nicolson, London.
Porter, B. (1989) *Plots and Paranoia: A History of Political Espionage in Britain, 1790-1988*, Unwin Hyman, London.
POST (1998) *Internet Commerce: Threats and Opportunities*, POST Technical Report 114, London, April.
Post Office Engineering Union (1980) *Tapping the Telephone*, POEU, London, July.
Poster, M. (1990) *The Mode of Information: Poststructuralism in a Social Context*, Polity Press, Cambridge.
Poulantzas, N. (1978) *State, Power, Socialism*, Verso, London.
Poulsen, K. (1999) "Wiretapping Abuses Alarm EFF, EPIC", *ZDNet News*, Sa Francisco, CA, 21 October, <http://www.zdnet.com/zdnn/stories/news/0,4586, 23781,00.html?chkpt=hpqsnewst> last accessed 25 October 1999.
PRCPP (1998) *Deconstructing Distrust: How Americans View Government*, PRCPP, Washington, DC.

Pugh, M. (1978) *Electoral Reform in War and Peace, 1906-1918*, Routledge & Kegan Paul, London.
Pye, L.W. (1963) "Communications and Political Articulation", in L.W. Pye (ed.) *Communications and Political Development*, Princeton University Press, Princeton, NJ, pp58-63.
Raine, G.E. (1920) *The Nationalisation Peril*, Thornton Butterworth, Ltd., London.
Ramsay, R. (1996) "The Influence of Intelligence Services on the British Left", *Lobster* Special Issue, Hull 1996 <http://www.lobster-magazine.co.uk/articles/rrtalk. htm>, last accessed 24 November 2000.
RAND Corporation (1992) *North Korea in the 1990s: Implications for the Future of the U.S.-South Korean Security Alliance*, RAND Note 3480, Santa Monica, CA.
Rheingold, H. (1993) *The Virtual Community: Homesteading on the Electronic Frontier*, Addison-Wesley, Reading, MA.
Richelson, J.T. (1986) *Sword and Shield: The Soviet Intelligence and Security Apparatus*, Ballinger Publishers, Cambridge, MA.
Ripley, R.B. (1966) "Introduction" in R.B. Ripley (ed.) *Public Politics and their Politics: An Introduction to the Techniques of Government Control*, W.W. Norton & Co., New York City, NY, ppvii-xviii.
Roberts, N. (1996) *Mobile Phone Crime: How Crime Related to Mobile Phones Can Be Recognised and Investigated*, Federation of Communication Services, London, December.
Robertson, J.H. (1947) *The Story of the Telephone: A History of the Telecommunicati-ons Industry of Britain*, Sir Isaac Pitman & Sons, London.
Robertson, K.G. (1982) *Public Secrets*, Macmillan, Basingstoke.
Rogers, A. (1997) *Secrecy and Power in the British State: A History of the Official Secrets Act*, Pluto Press, London 1997.
Rollins, N. (1992) "The Reichstag Method of Governing? The Attlee Governments and Permanent Economic Controls", in H. Mercer *et al.* (eds.) *Labour Governments and Private Industry: The Experience of 1945-1951*, Edinburgh University Press, Edinburgh, pp15-36.
Rolph, C.H. (1973) "The British Analogy", in P. Watters & S. Gillers (eds.) *Investigating the FBI*, Doubleday Company, Inc., Garden City, NY, pp387-411.
Romerstein, H. & S. Levchenko (1989) *The KGB Against the Main Enemy: How the Soviet Intelligence Service Operates Against the United States*, Lexington Books, Lexington, KY.
Rostow, W.W. (1960) *The Stages of Economic Growth: A Non-Communist Manifesto*, Cambridge University Press, Cambridge.
Rozell, M.J. (1994) *Executive Privilege: The Dilemma of Secrecy and Democratic Accountability*, Johns Hopkins University Press, Baltimore, MD.
Rozenblit, M. (2000) *Security for telecommunications network management*, IEEE Communications Society, New York City, New York.
Rubinstein, J. (1973) *City Police*, Farrar, Straus & Ciroux, New York City, NY.
Rule, J.B. (1973) *Private Lives and Public Surveillance*, Allen Lane, London.
Russell-Neuman, W. (1991) *The Future of the Mass Audience*, Cambridge University Press, Cambridge.
Russett, B. (1990) *Controlling the Sword: The Democratic Governance of National Security*, Harvard University Press, Cambridge, MA.

Sampson, A. (1973) *The Sovereign State: The Secret History of ITT*, Hodder & Stoughton, London.
Schramm, W. (1964) *Mass Media and National Development: The Role of Information in the Developing Countries*, Stanford University Press, Stanford, CA.
Schrecker, E. (1986) *No Ivory Tower: McCarthyism and the Universities*, Oxford University Press, New York City, NY.
Schwartz, J. (2000) "Court Says FCC Gives FBI Too Much Wiretap Power", *The Washington Post*, Washington, DC, 16 August.
Seabrook, M. (1987) *Coppers: An Inside View of the British Police*, Harrap, Ltd., London.
Sehgal, C. (2000) Electronic message addressed to Joseph Fitsanakis, ACLU, New York City, NY, 20 June (copy on file with author).
Seipp, D. (1977) *The Right to Privacy in American History*, Program in Information Resources Policy, Harvard University, Cambridge, MA, June.
Shaiko, R.G. (1998) "Reverse Lobbying: Interest Group Mobilisation from the White House and the Hill", in A.J. Cigler & B.A. Loomis (eds.) *Interest Group Politics*, Congressional Quarterly Press, Washington DC, 5th edition, pp255-282.
Shannon, L.W. (1958) "Is Level of Development Related to Capacity for Self-Government?", *American Journal of Economics and Sociology*, No 17, July, pp367-381.
Shannon, L.W. (1959) "Socio-economic Development and Political Status", *Social Problems*, No 7, January, pp27-43.
Shils, E.A. (1974) *The Torment of Secrecy: The Background and Consequences of American Security Policies*, Southern Illinois University Press, Carbondale, IL, 2nd ed.
Simpson, A. (2000) "Leaks and Plumbers", Washington Brief, Washington DC, 03 August, <http://www.wbrief.com/leaks.htm>, last accessed 20 November 2000.
Sims, C. (1999) *Consultation Paper on the Interception of Communications In the United Kingdom*, letter addressed to the Home Office's Organised and International Crime Directorate, West Midlands Police, Birmingham, 10 August (copy on file with author).
Slack, J.D. (1987) *The Ideology of the Information Age*, Ablex Books, Norwood, NJ.
Smith Group (2000) *Technical and Cost Issues Associated With Interception of Communications at Certain Communication Service Providers*, Smith Group, Ltd, London, 19 April 2000.
Smith, D.J. (1983) *Police and People in London. VIII: A Survey of Police Officers*, Policy Studies Institute, London.
Smith, I. (1999) *Interception of Communications in the United Kingdom: A Consultation Paper*, letter addressed to the Home Office's Organised and International Crime Directorate, UKERNA, Chilton, 12 August (copy on file with author).
Smith, P.T. (1985) *Policing Victorian London: Political Policing, Public Order and the London Metropolitan Police*, Greenwood Press, Westport, CT.
Smythe, D.W. (1954) "Some Observations on Communications Theory", *Audio-Visual Communications Review*, No 2, pp24-37.
Snape, T. (2001) "Concerns of Smaller ISPs", presentation given at the *12th ISPA Legal Forum*, London, 05 July.
Spencer, G. (1982) "Methodological Issues in the Study of Bureaucratic Elites: A Case Study of West Point", in R.G. Burgess (ed.) *Field Research: A Sourcebook and Field Manual*, George Allen & Unwin, London, pp23-30.

Spengler, J.J. (1963) "Bureaucracy and Economic Development", in J. LaPalombara (ed.) *Bureaucracy and Political Development*, Princeton University Press, Princeton, NJ, pp199-232.

Spiller, P.T. & I. Vogelsang (1996) " The United Kingdom: A Pacesetter in Regulatory Incentives", in B. Levy & P.T. Spiller (eds.) *Regulations, Institutions and Commitment: Comparative Studies of Telecommunications*, Cambridge University Press, New York City, New York, pp79-120.

Spindel, B.B. (1968) *The Ominous Ear*, Award House, New York City, NY.

Spitzer, S. (1985) "The Rationalisation of Crime Control in Capitalist Society", in S. Cohen & A. Scull (eds.) *Social Control and the State: Historical and Comparative Essays*, Basil Blackwell, Oxford, pp312-333.

Srinivasan, K. (2000) "White House Proposes Wiretap Law", *Associated Press*, Washington, DC, 17 July, <http://www.newsday.com/ap/topnews/ap957.htm> last accessed 17 July 2000.

Standler, R.B. (1997) *Response of Law to New Technology*, Concord, NH, 04 May, <http://www.rbs2.com/lt.htm> last accessed 04 February 1999.

Statewatch (1991) *Telephone Tapping* <http://www.poptel.org.uk/cgi-bin/> last accessed 25 July 1997.

Steinhardt, B. (1995) *What is the FBI Up To?*, ACLU, Washington, DC, December, <http://www.aclu.org/issues/security/oped.html> last accessed 13 May 1999.

Stewart, C. (1999) *Home Office Consultation on the Interception of Communications in the United Kingdom: BT View*, British Telecom, Plc., London, 18 August.

Stoddart, J. (1999) *IOCA Consultation Paper*, letter addressed to the Home Office's Organised and International Security Liaison Unit, Lincolnshire Police Headquarters, Lincoln, 02 August (copy on file with author).

Stone, A. (1989) *Wrong Number: The Breakup of AT&T*, Basic Books, New York City, NY.

Strum, P. (1999) *To Be Let Alone: Privacy in the United States*, ACLU, <http://www.aclu.org/aclu-e/salon/course5_strum1.html>, last accessed 24 March 2000.

STTCPUSHRCC (2000) *Hearing on Foreign Government Ownership of American Telecommunications Companies*, HR Hrg. 106-153, 106th Congress, 2nd Session, US Government Printing Office, Washington, DC, 07 September.

Sutter, G. (2001) "A Tale of Two Interception Regimes: RIP v CALEA, a Comparison", paper presented at the *16th BILETA Annual Conference*, University of Edinburgh, 09-10 April.

Taylor, D. (1997) *The New Police in Nineteenth-Century England: Crime, Conflict and Control*, Manchester University Press, Manchester.

Taylor, N. & C. Walker (1996) "Bugs in the System", *Journal of Civil Liberties*, 1(105), pp157-191.

Temin, P. & L. Galambos (1988) *The Fall of the Bell System: A Study in Prices and Politics*, Cambridge University Press, Cambridge, 2nd edition.

Tenet, G. (2001) Letter addressed to US Representative Stephen Horn, CIA, Washington, DC, 17 July (copy on file with author).

Teske, P.E. (1990) *After Divestiture: The Political Economy of State Telecommunications Regulation*, State University of New York Press, Albany, NY.

Theoharis, A. & J. Cox (1988) *The Boss: J. Edgar Hoover and the Great American Inquisition*, Temple University Press, Philadelphia, PA.

Theoharis, A.G. (1971) "Misleading the Presidents: Thirty Years of Wiretapping", *The Nation*, 24(212), 14 June, pp744-750.

Theoharis, A.G. (1978) *Spying on Americans: Political Surveillance from Hoover to the Huston Plan*, Temple University Press, Philadelphia, PA.
Thompson, E.P. (1968) *The Making of the English Working Class*, Penguin Books, Harmondsworth.
Thompson, V.A. (1976) *Bureaucracy and the Modern World*, General Leasing Press, Morristown, NJ.
Tivey, L.J. (1966) *Nationalisation in British Industry*, Johathan Cape, London.
Todd, P.A. (1999) *Consultation Paper on the Interception of Communications in the United Kingdom*, letter addressed to the Home Office's Organised and International Crime Directorate, Gloucestershire Constabulary, Cheltenham, 27 July (copy on file with author).
Toffler, A. (1980) *The Third Wave*, Pan Books, London.
Truman, D. (1958) *The Governmental Process*, Alfred A. Knopf Inc., New York City, NY.
Tsailovich, A.B. (1999) *Electromagnetic Shielding Handbook for Wired and Wireless EMC Applications*, Kluwer Academic, Boston, MA.
Tsang, D.C. (1998) "A CIA Target at Home in America", *The Los Angeles Times*, Los Angeles, CA, 18 January.
Tunstall, J. (1986) *Communications Deregulation: The Unleashing of America's Communications Industry*, Basil Blackwell, Oxford.
Turk, A.T. (1982) *Political Criminality: The Defiance and Defence of Authority*, Sage Publications, London.
UK Reference Services (1994) *Aspects of Britain: Telecommunications*, Central Office of Information, HMSO, London.
Ungar, S.J. (1975) *Federal Bureau of Investigation*, Little, Brown & Company, Boston, MA.
United States Court of Appeals (2000) *USTA v. FCC and USA Respondents On Petitions for Review of an Order of the FCC*, District of Columbia Circuit, Washington, DC, 15 August.
United States House of Representatives Committee on Government Operations (1987) *Report on the Computer Security Act of 1987*, House Report 100-153, Part 2, 100th Congress, First Session, Washington DC, 25, 26 February, 17 March.
United States House of Representatives Committee on the Judiciary (1975) *Impeachment of Richard M. Nixon, President of the United States*, Bantam Books, New York City, NY.
USCCGO (1974) *Telephone Monitoring Practices by Federal Agencies*, HR Hrg. 82nd Congress, Government Printing Office, Washington, DC, July.
USSSCSGORIA (1976a) *Intelligence Activities and the Rights of Americans: Final Report, Book II*, Report 94-755, 94th Congress, 2nd Session, Washington DC, 23 April.
USSSCSGORIA (1976b) *Supplementary Staff Reports on Intelligence Activities and the Rights of Americans: Final Report, Book III*, Report 94-755, 94th Congress, 2nd Session, Washington DC, 23 April.
USTA (1998) "USTA and Other Carrier Organisations File Petition with FCC to Resolve Wiretap Issues", USTA Press Statement, Washington, DC, 09 April, <http://www.usta.org/rls98-21.html>, last accessed 19 May 1999.
USTIA & USEIA (1997) *Lawfully Authorised Electronic Surveillance: Interim Standard Version*, J-STD-025, TR-45, Chicago, IL, November.

USTIA & USEIA (2000) *Lawfully Authorised Electronic Surveillance: Revised Version to Meet the Requirements Defined in FCC 99-230, CC Docket No. 97-213*, J-STD-025A, TR-45, Chicago, IL, May.

Veigas, H. (1999) *Consultation Paper on the Interception of Communications in the United Kingdom*, letter addressed to the Home Office's Organised and International Crime Directorate, Derbyshire Constabulary, Ripley, 27 July (copy on file with author).

Veigas, H.S. (2000) *Regulation of Investigatory Powers Act*, letter addressed to Joseph Fitsanakis, Derbyshire Constabulary, Ripley, 10 November (document on file with author).

Veljanovski, C. (1991) *The Future of Industry Regulation in the UK: A Report of an Independent Inquiry*, Lexecon, London.

Verrier, A. (1983) *Through the Looking Glass*, Jonathan Cape, London.

Verton, D. (2000a) "NSA Posts Declassified Intelligence from Korean War", *Federal Computer Week*, Falls Church, VA, 18 July, <http://www.fcw.com/fcw/articles/2000/0717/web-nsa-07-18-00.asp>, last accessed 20 November 2000.

Verton, D. (2000b) "Fighting Online Leaks", *Federal Computer Week*, Falls Church, VA, 31 July, <http://www.fcw.com/fcw/articles/2000/0731/pol-cia-07-3100. asp>, last accessed 20 November 2000.

Verton, D. (2001) "NSA Warns It Can't Keep Up With Rapid Changes in IT", *Info World*, San Mateo, CA, 19 February, <http://iwsun4.infoworld.com/articles/hn/xml/01/02/19/010219hnnsa.xml> last accessed 19 February 2001.

Vesely, R. (1997) "House Panel Questions FBI's Stance on Tap Law", *Wired News*, San Francisco, CA, 23 October, <http://www.wired.com/news/politics/0,1283,7932,00.html> last accessed 01 February 1998.

Virgo, P. (1999) *IMIS Draft Response to the Home Office Consultation Paper on the Interception of Communications in the United Kingdom*, letter addressed to the Home Office's Interception Legislation Team, IMIS, London, 13 August (copy on file with author).

Walker, C. (2001) "Encryption and the Regulation of Investigatory Powers Act 2000", paper presented at the *16th BILETA Annual Conference*, University of Edinburgh, 09-10 April.

Walker, J.T. (1997) "Re-Blueing the Police: Technological Changes and Law Enforcement Practices", in M.L. Dantzker (ed.) *Contemporary Policing: Personnel, Issues and Trends*, Butterworth-Heinemann, Boston, MA, pp257-276.

Ward, M. (2001) "Cybercops Arrest Online Liberty", *BBC News*, London, 18 April, <http://news.bbc.co.uk/low/english/sci/tech/newsid_1283000/1283127.stm> last accessed 18 April 2001.

Watson, D. (2000) *Regulation of Investigatory Powers Bill*, letter addressed to Joseph Fitsanakis, Lothian and Borders Police, Edinburgh, 14 August (document on file with author).

Weatherall, S. (1999) *Interception of Communications in the United Kingdom: Response by Unipalm Group Plc., Trading as UUNet*, UUNet, Cambridge, August (copy on file with author).

Weber, M. (1968) "The Essentials of Bureaucratic Organisation: An Ideal Type Construction", in R.K. Merton *et al.* (eds.) *Reader in Bureaucracy*, The Free Press, New York City, NY, pp18-27.

Weinberger, B. (1995) *The Best Police in the World: An Oral History of English Policing*

from the 1930s to the 1960s, Scholar Press, Aldershot.
West, N. (1983a) *A Matter of Trust: MI5 1945-1972*, Coronet, London.
West, N. (1983b) *MI6: British Secret Intelligence Service Operations, 1909-1945,* Random House, New York City, NY.
Westin, A.F. (1962) "Bookies and 'Bugs' in California: Judicial Control of Police Practices", in A.G. Westin (ed.) *The Uses of Power: Seven Cases in American Politics*, Harcourt, Brace & World Inc., New York City, NY, pp117-172.
Whitaker, B. (1964) *The Police*, Eye & Spottiswoode, London.
White, R. (1999) *Consultation Paper on the Interception of Communications In the United Kingdom*, letter addressed to the Home Office's Organised and International Crime Directorate, Powys Police Constabulary, Carmarthen, 23 July (copy on file with author).
White, T.H. (1975) *Breach of Faith*, Atheneum Publishers, New York City, NY.
Wigham, E. (1976) *Strikes and the Government, 1893-1974*, The Macmillan Press, Ltd., London.
Williams, R. (1974) *Television: Technology and Cultural Form*, Fontana & Collins, Glasgow.
Willing, R. (2000) "New Devices Prompt More Wiretapping", *USA Today*, 03 May.
Wills, G. (1999) *A Necessary Evil: A History of American Distrust of Government*, Simon & Schuster, New York City, NY.
Wilson, D. (1984) *The Secrets File: The Case for Freedom if Information in Britain Today*, Heinemann, London.
Wilson, K.G. (1988) *Technologies of Control: The New Interactive Media for the Home*, The University of Wisconsin Press, Madison, WI.
Wingfield, J. (1984) *Bugging: A Complete Survey of Electronic Surveillance Today,* Robert Hale, London.
Wise, D. (1973) *The Politics of Lying: Government Deception, Secrecy and Power*, Vintage Books, New York City, NY.
Wise, D. (1976) *The American Police State: The Government Against the People*, Random House, New York City, NY.
Wolmer, V. (1932) *Post Office Reform: Its Importance and Practicability*, Ivor Nicholson, London.
Woods, B. (1993) *Communication Technology and the Development of People*, Routledge, London 1993.
Wraith, J., (2000) "Law Enforcement Issues", presentation given at the *Telecommunications United Kingdom Fraud Forum Annual Meeting*, London, England, 12 April (copy on file with author).
Wright, P. (1987) *Spy Catcher: The Candid Autobiography of a Senior Intelligence Officer*, Stoddart Publishers, London.
Yarbrough, D. (1999) *Declaration Before the Federal Communications Commission in the Matter of CALEA*, CC Docket No 97-213, Washington, DC, 27 January.
Yarbrough, D. (2000) *Communications Assistance for Law Enforcement Act*, FBI, CALEA Implementation Section presentation, Chantilly, VA, October 2000 (copy on file with author).
Zuboff, S. (1988) *In the Age of the Smart Machine: The Future of Work and Power*, Heinemann, Oxford.