

MISUSE OF COMPUTERISED PERSONAL FILES -
LEGAL AND TECHNICAL CONSIDERATIONS,
WITH PARTICULAR REFERENCE TO CERTAIN APPLICATIONS
OF REAL-TIME SYSTEMS IN LOCAL GOVERNMENT

Submitted for the degree of Doctor of Philosophy
of the University of Aston in Birmingham

Andrew Charles John Hawker.

The research described in this thesis was carried out
with the aid of a studentship of the Science Research Council

April 1974

177345 .14 OCT 1974

THESIS

343.45
HAW

SUMMARY

The thesis describes the use of personal information by local authorities in their routine administration, and extrapolates some conclusions about problems of processing this information in a computerised environment of the future.

A model of privacy-risk situations is presented. The aim of this is to provide a basis for legal and technical analysis, by representing both human and technical factors.

The law relating to privacy of information, the state of the art of techniques for controlling access to computer-stored information, and the role of information processing in local authorities, are each surveyed.

Detailed studies of current practice in handling personal information are given in four areas, namely: Social Services, Housing, Education and Finance.

Proposals are made for a combination of legal reforms and technical measures which would safeguard the interests of the individual about whom data is stored. Central to these is the idea of a "privacy label", used in conjunction with dispersed centres of control within the information system.

A NOTE ON THE ORGANISATION OF THE THESIS

Each chapter is divided into numbered sections, and these are occasionally further divided into sub-sections.

Where a figure such as "4.4.2." is quoted without any qualification, this should be taken to refer to sections 4.2 of chapter 4.

The references for each chapter are listed at the end of the main text, marked by a pink sheet in the binding. Reference is always by number, thus: (21).

Footnotes are indicated by lower case letters in brackets, thus: (c).

Contrary to normal legal practice, cases and statutes are indexed at the end of the thesis.

Some words have been used with both their legal and technical meanings in the thesis (for example, "privilege"), and a Glossary attempts to define the meanings to be attributed to these and other key words.

A complete list of contents follows on the next page.

Legal note: the law is stated as at 1st November, 1973.

C O N T E N T S

		Page
	Thesis summary	
	Organisation of the thesis	1
	Acknowledgements	4
	Introduction	6
 <u>PART I</u>	 <u>Review of the problem area, and presentation of a model of privacy-risk situations</u>	
	Preface	13
	Chapter 1 The debate about privacy	14
	Chapter 2 A general model of privacy-risk situations	23
	Chapter 3 Legal survey	42
	Chapter 4 Technical survey	83
	Chapter 5 Local government survey	104
 <u>Part II</u>	 <u>Empirical studies of the use of personal information in local government, with special reference to Birmingham</u>	
	Preface	118
	Chapter 6 Social services	120
	Chapter 7 Housing	142
	Chapter 8 Education	176
	Chapter 9 Rating and Finance	186
	Chapter 10 Conclusions from the studies	197

Part III Proposals and general conclusions

Preface	200
Chapter 11 Technical proposals	201
Chapter 12 Legal and administrative proposals	218
Chapter 13 Conclusions	248
References to Chapters 1 - 13	254
Glossary	269
Appendix I USA official references	271
Appendix II Areal units in Birmingham	273
Appendix III Sample privtype transaction	275
Bibliography	278
Index to cases	289
Index to statutes	294
Index to subjects	296

ACKNOWLEDGEMENTS

Three organisations in particular have given me generous assistance in preparing this thesis.

Firstly, the University of Aston, through its Interdisciplinary Higher Degrees Scheme, provided the opportunity to tackle an absorbing but rather nebulous subject, and to try to establish some ground-rules for it. This permitted a freedom of approach which is not the norm of post-graduate research, and the IHD Scheme took a number of risks in launching the project. I hope the credit for taking such risks will survive the shortcomings which will certainly be found in the thesis which follows. There are always safer horses to back in the research field, and I would like to thank Dr. Alastair Cochran, George Lindfield, Dr. Ruth Montague, and Professor S.L. Cook for their continued commitment to the project.

Secondly, the Scientific Centre of IBM (UK) Ltd acted as industrial sponsors of the project. The involvement of a leading computer manufacturer will no doubt raise some spectres of a "whitewash" job for the computing industry. I hope anyone tempted to such a judgment will first read the comments about the industry, and indeed about some IBM publications, in the thesis. IBM have provided invaluable help in keeping my feet on the ground as to the state of the art of data processing. At no time has the company suggested that any conclusions would be preferable, or any aspects of the subject best avoided, and indeed the company's representatives sometimes found themselves advocating a more open-ended approach than the university supervisors. I am indeed indebted to the many IBM employees who committed their time and resources to helping the research, and particularly to the three people directly associated with the project, namely: Pat White, Dr. Garth Notley and Dr. Ken Hanford.

Thirdly, the Corporation of Birmingham, through its officers in Social Services, Housing, Education, Treasurer's, and other departments, allowed me to study the use and processing of personal information at first hand. The officers, quite rightly, were at pains to ensure that my own investigations should not intrude on anyone's privacy, and this often meant extra work on their part. A great many clerical staff put up with questions about, and observations of, their routine work, and did so most hospitably. All this was at a time of continuing internal reorganisation, with the new structure of local government being imminent, and so I am most grateful to all concerned.

For the rest, I owe a great deal to the large number of individual people who have provided comment and information over the past three years. I am especially grateful to Professor Selmer, Jon Bing and Ragnar Blekeli, who laid on a fascinating study week at their Center for Computers and the Law, in Oslo; to T.R.H. Sizer, and other members of the British Computer Society, who have been pegging away at this subject much longer than I have; to the officers of the Camden, Coventry, Kent, Mansfield, Nottinghamshire and Tower Hamlets local authorities, who explained their information systems in some detail; to R.C. Sanderson of LAMSAC; Michael Stone of West Sussex County Council; G.F.P. Boston of the Titchfield Census Office; and G.F. Atherton of the Police National Computer Unit.

In the academic world, people who kindly gave their time to discuss the subject included: Jim Baxendale (Rutgers University), A.J. Beith (Newcastle University), R. Denenberg (Swansea), J.M. Jacob (L.S.E.), Dr. G.B.F. Niblett (UKAEA), Dr. J.B. Rule (New York State University), and Colin Tapper (Oxford). In addition, I had innumerable useful discussions with staff and fellow students at Aston.

All the errors in the thesis are of course there in spite of the expert advice from all these sources, and no part of the thesis should be regarded as representing a view held by anyone in the preceding paragraphs, unless this is expressly stated to be the case.

Andrew Hawker.
14th March 1974.
University of Aston in Birmingham.

INTRODUCTION

1. Preliminary definitions

How can one "misuse" personal information? In the broadest sense, misuse could comprise libel, blackmail, or a number of illegal activities. This thesis is concerned with the misuses which are associated with "invasion of privacy". However, "invasion of privacy" has become an emotively favourable way of denoting a number of different threats to individual dignity and autonomy. Particularly in respect of the new technology of computing, the phrase has proved a useful, ad hoc, label with which to designate a problem area whose characteristics have been and still are forming.

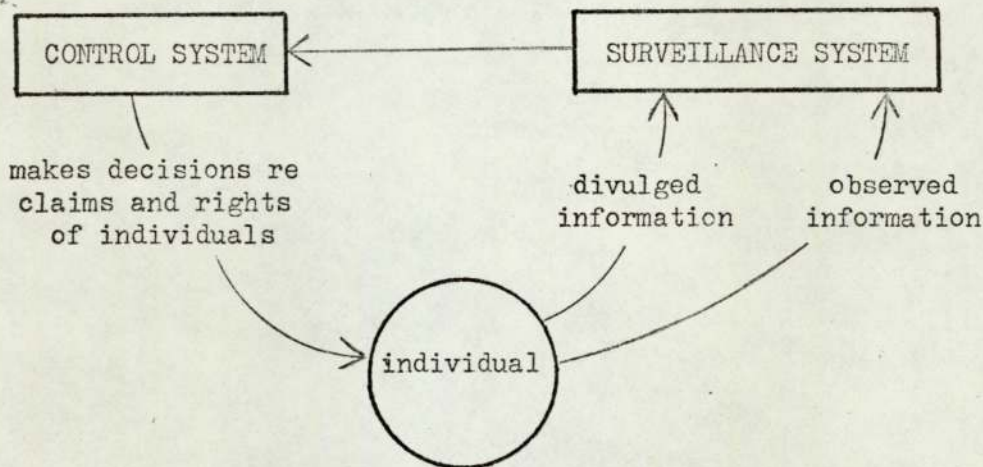
Furthermore, in considering the question of "privacy" in the context of computers, local government and the law, it quickly became evident that the word had chameleon-like qualities. It would blend in with all the attitudes, preoccupations and expectations of the group of people using it. Thus for computer analysts, "privacy" is a functional word, covering anything to do with controls over access to data. The compass of the word may even be extended to technically related questions of protection against data loss or corruption. For local government officers, "privacy" has political overtones, since the collection and dissemination of information must be in furtherance of some administrative policy, in which the role of the officer or department may be an integral issue. For them, privacy is just one of several factors to be considered when collecting or passing on information. Lastly, the lawyers tend to concentrate on the rights or claims of the individual. In the absence of any legal right to privacy under English Law, lawyers have to approach the subject indirectly, specifying other rights which can be invoked in order to effect privacy

protection. The lawyer is also concerned with the nature of each organisation within which the computer is to function, since a lot follows from this about the responsibilities of the organisation and the sanctions which can be invoked against it.

These different interests are not all directed at the same problem; still less do they result in answers which are compatible with one another. This preliminary chapter, therefore, attempts to set down the problem which is under consideration in the rest of the thesis. Various answers are then suggested in the thesis, and it is for the reader to judge their merits. However, a major objective has been to make proposals which best exploit a concerted effect of legal, political and technical measures implemented together. Anyone assessing the proposals purely in terms of legal reform or technical innovation will be dissatisfied and disappointed.

2. "Invasion of privacy"

A very simplified picture of those privacy-risk situations likely to involve computers is as follows:



In this figure:

A "control system" is some means of influencing the behaviour or situation of the individual, and a "surveillance system" is an information system which assists the exercise of this influence: (the terms are used in the senses proposed by Rule)(1).

"Divulged information" is that which the individual consciously provides to someone else, while "observed information" is that which is obtained without the knowledge of the individual.

"Rights" are defined in the legal sense, as being complementary to obligations or duties: if the obligation or duty is proved with regard to the individual, the law will insist that his right be respected. "Claims" on the other hand include all benefits which the individual may seek, but where the law allows discretion as to whether the claim is to be met. So for example someone may have a right to a rent rebate but only a claim to be allocated a council house.

The individual is very much a part of this picture: his view of how well his privacy is being respected will be restricted by his enclosure in it. However, there are various reservations he may have about the effects of the system as a whole. He may, for example, have objections to:

- (i) the means by which observed information has been acquired
- (ii) the form or scope of the information about him stored in the surveillance system, at any given time
- (iii) the kind of people who can retrieve the information from the surveillance system
- (iv) the decisions made in the control system

Opinions vary as to whether all these objections are rooted in a desire for "privacy". Some writers, such as Benn, (2) concentrate on the sense of affront occasioned by invasion of privacy - an important consideration in (i) and (iii) above. He speaks of "... a resentment that anyone - even a thoroughly trustworthy official - should be able at will to satisfy any curiosity, without the knowledge let alone the consent of the subject". (3) In these terms, resentment of intrusive scrutiny does not involve any fears about the consequences (as in situations where someone wishes creditable information to be treated as private). The analysis therefore centres on the actual act of intrusion.

Other concern derives from the political implications of surveillance systems. The fear is that the control system will become despotic, by virtue of the facility which the surveillance system provides for identifying people who deviate from certain behaviour patterns. This has led sociologists such as Rule to examine the mechanism of surveillance and control, with the aim of identifying some of the characteristics which will make for a healthy political situation. Similarly, studies at the Norwegian Research Center for Computers and Law have tried to identify those administrative practices which encourage respect for privacy. (4) The emphasis here is on the role of personal information in decision-making and the consequences for the individual.

The threat to the individual from this misuse of information is to his personal freedom, or autonomy; there may also be intrusions into privacy, but not necessarily so. The dividing line again depends on the scope one is willing to allow to "privacy". The distinction has been discussed by Beardsley, (5) but the question will be dodged for the purpose of this thesis, since in practical terms the protection sought by the individual will be similar, whether he frames his objections in terms of privacy or

autonomy. He will assert a claim to influence the decisions, however and whenever taken, whereby information about him is made available to other people. The strength of his claim will have to be assessed on the basis of political considerations. The strength of his actual influence will depend on various factors, not least being the ability to establish what is going on inside the surveillance system. Hence the issue is inextricably linked to other questions of permitting access and enforcing secrecy in public administration - a field which has, Lowry suggests, (6) received comparatively little attention from researchers.

This latter kind of interest will be termed for convenience "pragmatic", and the former interest, centring on the conduct of the intruder, "ethical". This division of interest is by no means neat or clear-cut, but it does facilitate some observations on the impact of the computer.

Firstly, although a computer cannot make ethical judgments, when an administrative procedure is automated, some automatic substitute for such judgments may have to be built into the system. For example, whereas dependence has previously been put on the discretion of individuals in not revealing information passing through their hands, the equivalent computerised procedure may be protected by logical and hardware controls over output. The ethical problems change rather than disappear. A different group of people will now have a different mode of access to that same information. For these people, the scope and opportunity for exercising curiosity may change, and we may have to reformulate ideas on what constitutes unethical behaviour on their part.

Secondly, the computer has two important effects on the information it processes. It makes it possible for the information to be very widely and

easily accessible; and it disassociates the information from its original context. The two effects are closely related, since the distributive power of a computer system depends on its ability to store and transmit information in standard codings, as data. Such data may be a bit-stream carrying no clues about its origins. As with dehydrated soup its reconstitution as information may leave wide scope for the imagination as to where the ingredients came from. This again has relevance to ethical judgements, since we cannot blame people for not respecting privacy norms, if they are not given the necessary cues to work by.

But it is the distributive and integrative power of the computer which mainly alarms the pragmatists, since this can be so readily exploited for surveillance systems. The basis of the alarm is not necessarily the actual obtaining of information about each individual, which may be quite unobjectionable if taken in isolation. But the ability to draw together all the inputs to the system confers power which can be exercised in a number of ways. Firstly, pressure can be brought to bear selectively on individuals. Discrepancies or deviations which are commonplace, but perhaps not readily admitted, can be used to discredit or embarrass someone. Secondly, if the system is used in determining entitlement to benefits, the availability of a wide range of information makes it possible to make discriminations in awarding the benefits, using grounds which are biased and irrelevant. Similarly, pressures of the kind described in the first example can be applied against people selected by objectionable criteria, such as race or religion. Thirdly, records of overtly anti-social behaviour can be stored and distributed to an extent whereby so many decisions are weighed by them that a "snowball effect" of punishment is created. Lastly, a surveillance system can be used to protect its own existence and the interests of those who operate it. By monitoring

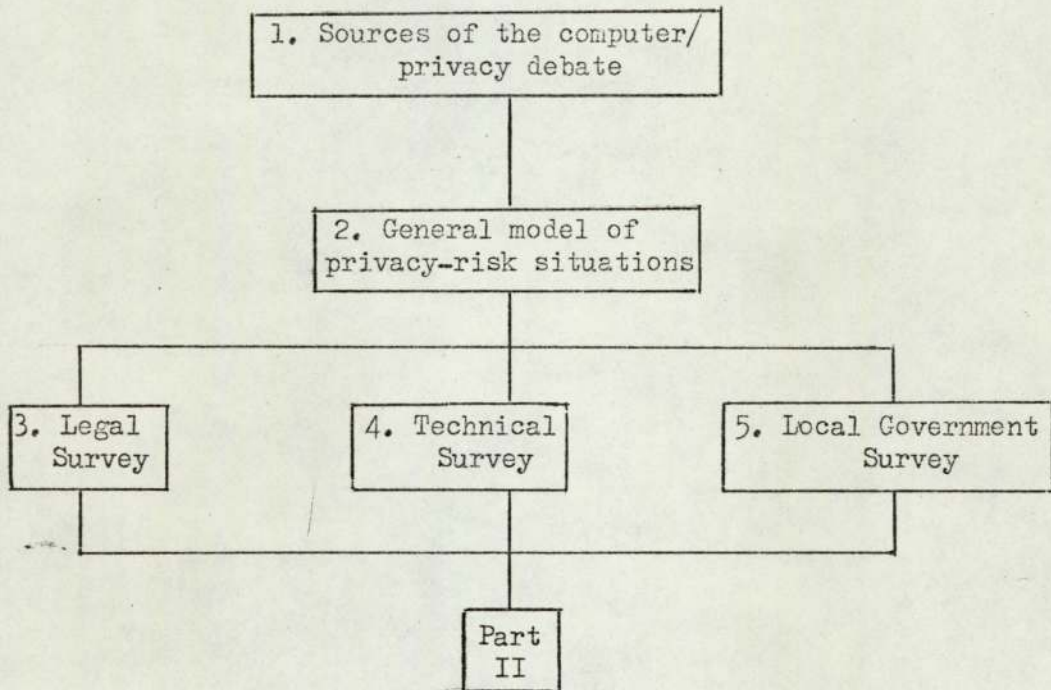
anything felt to be threatening, the operators of such a system may be able to outflank their critics and court popularity.

None of these effects follows inevitably from the creation of a surveillance system. Many surveillance systems exist already, and are operated to the general good of everyone. But it is wise to inquire whether the computer is likely to upset the balances which ensure this state of affairs. We have a great capacity for surprise at the impact of new technologies, and in this case we can particularly ill afford to stand and stare while social mechanisms are created which have an ominous streak of self-preservation built into them.

PREFACE TO PART I

The aim of Part I of the thesis is to outline the origins of the computer/privacy debate; to extend the model of privacy-risk situations, mentioned briefly in the introduction; and to present salient information drawn from the legal, technical, and local government literature.

The reader is asked to treat Part I as a means of setting the scene for the rest of the thesis. At this stage the chapters are not intended to follow closely one on another. Their pattern is:



The aim has been to make all chapters easily comprehensible to a general readership. However, a certain amount of jargon proved unavoidable in chapters 3 and 4: a glossary is provided for some of the terms, together with those defined in chapter 2, at the end of the thesis.

CHAPTER 1REVIEW OF THE COMPUTER-PRIVACY DEBATE1. History

In 1949, George Orwell cast a pessimistic eye on the future and made 1984 a memorable year before it had even arrived. His book is unique in many respects. Though futuristic, it has none of the scientific trappings of Huxley or Wells, (in fact, advances seem to have been up a very few cul-de-sacs, in creating huge war machines, the Newspeak speakwrite, and the ubiquitous telescreens). It is very much a book of its time, dealing with power-blocks, brain-washing, and the huge bureaucracies which were among the legacies of World War II. Yet Orwell's key elucidation, of a relationship between power and privacy, transcends the setting of the book. Everyone is governed not by political process, but by the fear that a single move may be noted and construed as opposition to the policy of the moment. Policies change, history changes, reality is what the total information system determines it to be. Orwell nowhere mentions computers, which in his time were still vacuum-tube prototypes, but their eventual application in the Ministry of Truth would seem to be a foregone conclusion.

Back in the real life of 1949, democracies were adjusting to a cold war in which the rules governing intrusion in the public interest had to be a good deal more elaborate than they had been during open hostilities. In America, suspicions of Communist subversion grew to the point that suspects could expect to have every detail of their lives bared to public view; the effects of the hysteria on attitudes to privacy were later analysed by Edward Shils. (1) In England there were anti-communist scares on a smaller scale in the early 1950's, leading to the establishment of a Conference of Privy Councillors in 1955 and a White Paper in 1956. (2) A year later, the particular issue of telephone tapping was investigated by another group of privy councillors under Lord Birkett. (3) Security procedures in the public

service were further reviewed by the Radcliffe Committee in 1962. (4)

Away from this intensely political arena, concern was growing at about the same time over the freedom with which the press, and its new rival television, could intrude on someone's private affairs without incurring liability (so long as statements made were not defamatory). In 1961, a Right of Privacy Bill was introduced by Lord Mancroft. (5) This provided a remedy if a publication or broadcast was calculated to cause "distress or embarrassment". The Bill was supported by eminent Law Lords, and in an article published some months later in the Modern Law Review. (6) However, after this first foray the subject was destined to languish for five years or so.

In America, meantime, plans were afoot to integrate a wide range of government statistics on computer tapes. A task force of the Bureau of the Budget reported in 1966, (7) and their ideas ran into strong adverse criticism. Later in the same year, the House Committee on Government Operations held public hearings on the matter, with the proponents of the National Data Center put very much on the defensive by hostile questioning from the Committee. (8) The full story of the National Data Center has been described elsewhere, (9) but notwithstanding the continual enthusiasm for the idea on the part of the leader of the task force, (10) official approval did not materialise. Comment on the other hand, continued for some time afterwards, (11) mainly deprecating the proposals.

In the absence of such a proposal in this country, opinion against the "databank society" was slower to mobilise. Credit for being one of the first to anticipate this particular debate is due to Professor M.V. Wilkes, who, outlining some of the possible developments, in 1964 concluded: "Many branches of life will lend themselves to continuous computer surveillance, and I leave it to the readers to decide whether or not this is a pleasant

prospect!" (12)

Most of the debate about computers, however, centred on automation, and the threat which this implied to full employment, rather than privacy. Thus a reassuring and often optimistic picture was painted by the Chairman of Elliott-Automation Ltd in the 1964 Reith Lectures. (13) Automation was also a dominant concern in the popularising books about computers which now began to appear. The development of large networks and facilities for machine-coded data exchange would typically be discussed as a promising possibility in just a paragraph or two. (a) Computers as data retrieval devices began to assume a more menacing aspect towards the end of the decade, at which time a marked "anti-technology" swing in the mass media was becoming apparent. Thus one of the leading "doomsday" books published in 1969 included references to the computer's threat to privacy, (14) and press interest was stimulated by the introduction by Kenneth Baker, M.P., of his Data Surveillance Bill in May of that year. (15) Political interest had already been shown by Mr. Baker's party, in the publication of a research paper late in 1968. (16)

(a) "... there is no doubt that every citizen will be given an identifying individual reference number upon birth and that this number will enable all details about him or her to be maintained by Government from the cradle to the grave. With one code number for every purpose, our life would be very much easier." B. Murphy, "The Computer in Society, Blond, 1966, at p.1015; see also J. Hargreaves, "Computers and the Changing World", Hutchinson, 1967, (particularly at p.118-119, where information networks are discussed in more general terms.)

Interest on the wider privacy issue was also growing. Right of Privacy Bills were introduced in 1967 and 1969, (the latter leading to the establishment of the Younger Committee). (17) The issue was also being pressed by the National Council for Civil Liberties, which in 1968 published a lengthy pamphlet on the subject. (18) Justice (the British Section of the International Commission of Jurists) had set up a committee on privacy, following an international conference on the subject in Stockholm in 1967 - the committee's report was published in 1970. (19)

2. Sources of the current debate

2.1. Overseas. After the 1966 Gallagher Hearings in America, (8) inquiries proceeded into various aspects of the use of computer databanks. A list of these proceedings is given in Appendix I. Reports published by Professor A.F. Westin in 1967, 1971 and 1972, (20) as well as numerous articles, (21) established him as a leading authority in the field.

International organisations such as O.E.C.D. (22) and the U.N. (23) have also sponsored reports relating to computer privacy.

2.2. Great Britain.

2.2.1. Law. A leading campaigner on the issue in the late 1960's was a London law lecturer, Joe Jacob. (24) He was one of the first people to press for strong regulation of databanks, as opposed to the registration envisaged under the Data Surveillance Bill, and the Control of Personal Information Bills introduced subsequently by Leslie Huckfield, M.P., incorporated his ideas.

Other researchers concerned with legal-computer issues have included privacy in their remit, including Dr. G.B.F. Niblett of UKAEA, (25) and Colin Tapper of Magdalen College, Oxford. (26) Interest among non-academic lawyers has tended to be expressed through organisations such as Justice, or the party political lawyer groups. Some lawyers have of course contributed to the parliamentary process itself. (b)

2.2.2. The Computer Industry. The computer press has reported and discussed the privacy issue at some length (more so than the equivalent legal professional journals), and privacy has been a major concern of the British Computer Society. Sources of concern vary. Manufacturers and bureaux are faced with additional costs in providing privacy protection. Computer users in turn tend to look over their shoulders to the consumers, (c) i.e., the people about whom they store data and whose expectations about privacy may not be all that clear.

The BCS has published guidelines on privacy, (27) but at present the Society lacks any real authority with which to require that the standards it proposes should be followed throughout the industry.

2.2.3. Political pressures. "The Databank Society" was pushed into the limelight by the National Council for Civil Liberties in November 1970, when it organised a two-day conference under this title. (28) The tone of the conference was fairly alarmist, with Professor Westin and Congressman

(b) e.g., Lord Gardiner, House of Lords Hansard Vol 343, 6th June 1973, at col. 125.

(c) later to be defined for convenience as "indids" - the individuals identified in the data. (see chapter 2 on "Concepts")

Gallagher foremost among the delegation from America. Few doubts were cast on the ability of computers to underpin powerful surveillance systems within quite a short time-span. (d) The conference was timed to coincide with the publication of "The Data Bank Society" by Malcolm Warner and Michael Stone. The book, also, derived a good deal from the American experience, and must be seen now as the means of awaking people to an important subject, in much the same way that Rachel Carson's book "Silent Spring" triggered debate about pollution of the environment. As with pollution, the problems, and especially their solutions, are turning out to be more extensive and complicated than could have been apparent at the time they were first recognised.

The criticisms made at the NCCL conference of the Younger Committee's inability to consider the public sector, coupled with the extensive publicity surrounding the conference, (29) proved sufficient leverage for the Prime Minister to refer the privacy of government records for study by the Civil Service Department. However, the CSD's findings have not been published. (30)

The conference also paved the way for intensive debate of computers and privacy in the first few months of 1971. In February, Leslie Huckfield introduced his Control of Personal Information Bill, (31) and shortly afterwards the first reports began to appear of the investigation of personal files kept by the American Defense Department, led by Senator Sam Ervin. (32) However, the biggest storm was brewing for the Decennial Census, due on 25th April. The fuss, (33) which came as something of a

(d) Rex Malik, technical journalist, was the only speaker seriously to question the feasibility of some of the systems envisaged (author's notes of conference).

surprise to census personnel, and in some instances was justifiably resented, (34) led to the institution of study groups from the BCS and the Royal Statistical Society, to look into census security. Their reports (the BCS contribution looking extremely emaciated, supposedly for security reasons) appeared over two years later. (35) M.P's., Leslie Huckfield and Arthur Lewis foremost among them, continued to raise the subject for some time afterwards. (36)

Shortly after the Census representatives of the BCS appeared before the Science and Technology Sub-committee "A" for the second time, and their evidence now contained several references to privacy. (37) On 25th May, the first meeting was held of the BCS's newly-formed Privacy and Public Welfare Committee, which took over from the Society's Privacy Committee, with a more influential status within the Society.

The "Guardian" had, meanwhile, given the topic of government record-keeping another prod with a front-page article headlined "Commercial spies tap State records". (38) The story was taken up at question time by Leslie Huckfield, (39) and further inter-departmental enquiries were promised. No results of these enquiries have been published. (40)

On 1st June, the "Guardian" published a further story outlining the dangers of computer systems in school administration, and the subject was raised in parliament by Mr. Huckfield. (41) However, apart from an adjournment debate initiated by Mr. Huckfield on 27th July, (42) little further debate attended the computer/privacy issue, in the Press or Parliament, during the rest of 1971.

3. The Younger and Franks Committees

The reports of these committees were published in July and September 1972, respectively. (43) Neither committee had local government within its terms of reference, but both made observations on security and confidentiality which will be discussed later in this thesis.

The Younger Report has been the subject of two Parliamentary debates, (44) and the rejection by the majority of the committee of the idea of a general right of privacy came in for criticism. (45)

4. Conclusions

Lest the preceding survey give the impression that opinion has formed staunchly against computer stores of personal information, it should perhaps be emphasized that many intermediate and even opposite views are held. These views, especially where they belong to civil servants or local government officers, rarely find their way into print. However, on several occasions the author was presented with very cogent criticisms of the conventional wisdom on computer privacy. That these criticisms have not had wider attention is partly due to a commendable tradition that public officers do not involve themselves openly in contentious political issues. However, in the case of the civil service particularly, a secretive urge which can only be described as obsessional does a disservice to the civil servants' case and the cause of informed public debate.

Two instances of a countervailing philosophy can, however, be instanced. In the wake of the Gallagher Hearings in the USA, C.C. Bennett questioned whether privacy was as inalienable a right as it had been made out to be: (46) and in a review of A.F. Westin's "Privacy and Freedom",

F.H. Newark wrote: "If the A organisation has data lawfully acquired about one aspect of John Doe's activities, and the B organisation has other data lawfully acquired on the same John Doe's activities, there is nothing illicit in their pooling the information. And if thirty other organisations join in and all the information is put into the computer, even though it means that an awful lot is known about a lot of people's activities, it is difficult to see on what principle the operation can be condemned." (47)

Such is the null hypothesis from which this thesis must begin.

CHAPTER 2

A GENERAL MODEL OF PRIVACY-RISK SITUATIONS

1. Introduction

This chapter proposes a simple model with which to view the movement of personal data processed by computer systems. The terminology of the model is used later in the thesis, particularly in making proposals for legal and technical safeguards. (Part III)

The model is put forward merely as an aid to analysis. It is envisaged that if such privacy analysis were applied in connection with a proposed or actual system, considerable elaboration of the flow diagrams would be necessary.

2. Models in Computing and in Law

In the computing world, a "model" is usually used to simplify and quantify a real-life situation, in order that changes in the state of the real world can be simulated, and the repercussions of change can be analysed or perhaps predicted. Particularly in computer-based simulation, it is expected that the model will be an imperfect representation of reality, capable of providing only limited (ie., generalised or probabilistic) conclusions.

Lawyers sometimes model situations, but in a different way. In order to illustrate a point of legal argument, it may help to identify a characteristic set of circumstances. For example, one might describe a sequence of events involving persons A, B and C. This modelling tries to identify the particularly salient points about a situation - often incorporating qualitative factors such as motive or intention.

The model outlined in the following pages is a development of this second kind of model, but ideas for diagrammatic representation have been borrowed from the computer world. It is conceivable that extremely complex privacy-risk situations may one day be simulated by computer processes, but nothing so ambitious is proposed here.

3. Definitions

It is helpful to try to model the various situations which can arise, in which the manipulation of information by a computer system can put a person's privacy at risk. But first, a number of definitions must be attempted. What, for example, do we mean by "a system"? It is generally acknowledged that the scope of a system is "what you choose to look at": just as one can consider the economic system at the level of the state or the supermarket. At present, a computerised information system can usually be identified with a hardware configuration within a given organisation, but future situations are likely to be complicated by the growth of schemes for networked and shared facilities. In LOLA (1) for example, one computer serves four local authorities. So do we have four information systems or one? The technical advantage was seen to be with creating one system. However, each of the four authorities retains a separate political status, and four sets of departments use the facility.

The characteristics of systems - their "strata", "layers" and "echelons" - have been analysed in depth by Mesarovic. (2) Of these concepts, the echelon is perhaps the most useful for privacy analysis. An echelon describes a "layer" in the system which accepts directives from above, but which retains its own autonomy, and can disregard the directives if this seems desirable. This is the essence of most human authority systems. Computer systems, on the other hand, do not mirror

this pattern. An operating system must be able to intervene immediately a subordinate program steps out of line, otherwise the whole system will come to a confused halt.

For this reason, it is usually easy to identify a centre of control for a computer system. For human systems, it is rarely as easy. To define a "system" for practical purposes, it is necessary to take account of both the computer's authority-structure and the organisation's authority-structure. A working definition is proposed: where an organisation is autonomous in determining its policy regarding the storage and dissemination of personal information and where it has substantial control over the computer facilities in which such information is processed, then the information will be regarded as flowing within a single system.

THE FOUR PERSON MODEL

With regard to our system, we can now define four persons by role. Strictly speaking, a "person" can either be an individual or an organisation. However, since the privacy rights of these two kinds of person differ (and may even conflict), the present analysis will tend to view persons as individuals: qualifying comments with regard to organisations will be made, as appropriate.

The four persons are:

1. INDID. A person about whom information is stored in the information system. Thus we have a large set of persons, many of whom are likely to be indids with respect to several different items of information. It will be convenient to refer to such items as "indid-data".

2. USER. A person having reasonably ready access to data in the system. Someone actually operating a terminal would clearly be included, but in some situations it may be that X does the mechanics of retrieval and passes the data straight over to Y. Y might then be the user rather than X.

3. COLLECTOR. A person, responsible for entering the indid-data into the system. This again may involve two or more stages, and it may be convenient to designate as "collector" an individual who supervises a group of people handling data input.

4. HOLDER. A person having control over the system as a whole. In accordance with preceding remarks, it may be difficult to identify one person exercising this control, but it would typically be the owner or director of the organisation using the computer-based data system.

4. Types of Privacy Infringement

4.1. A distinction has to be made between divulged and observed information. This depends on the ultimate source of the information. If the indid communicated the information to someone else, he had some control over how and when the information flow began: he "divulged" the information. If, on the other hand, someone eavesdropped on his conversation with a spy microphone, the information was obtained by observation, even though it may have been simultaneously divulged to someone in the same room.

We can then imagine an information "chain" from the source, via the information system, to the user. This could get quite complicated, as the

information could be passed from person to person, or re-observed. Two particular complications are:

1. the information may change substantially as it passes along the chain. People may add inferences, or alter the context, or simply get it wrong.
2. the information may relate to more than one individ. If, for example, X states "I committed a fraud with the aid of Y", the information could be stored by reference to either X or Y. This is an aspect of a wider problem, discussed later. However, two qualifying rules are required to counter these two difficulties:
 - * if the information changes substantially, we consider a new (presumably false) item to have begun at the next point in the chain:
 - * if information is of the form "X is related to Y", then two distinct items of information exist from the point of view of privacy protection. One is "X is related to Y", where the information originated from X or from source close to him; the other is "Y is related to X", where the chain originated from Y. In either case, the statement could be divulged or observed, but a divulged statement "Y related to X" can be construed as an observed statement "X related to Y".

A further complication arises when the same information item passes along two different chains to be input to the same information system. In one sense, the information is validated; but its privacy implications may

be obscured. The general rule should be that the stronger privacy condition should apply, unless a waiver is associated with one form of the item, and this form post-dates the other.

4.2. There are essentially four factors in any privacy-invading situation. They are more or less independent of one another.

4.2.1. CIRCUMSTANCES. Ideally, one would consider all the circumstances having any connection at all with the information-chain. However, the circumstances we shall be mainly concerned with are those implying that more than usual privacy protection should be provided, and which the collector knew about, or which a reasonable person would have expected to apply (a test which is familiar in law). (3)

4.2.2. NATURE OF DATA. This may be unambiguous, eg., in a plain text statement such as "X has an income of £2000 p.a." However, the data may be interpretable only in context, as for example where a name appears in a list of people who have an attribute in common. The data may be "secondary" or "tertiary" in the senses proposed by Sundgren, (4) ie., the user must connect together other information from the system or from his own memory in order to deduce its full meaning.

Data may also be significant because it links together other data: thus the data "A123: Z789" may appear innocuous, until it is discovered that the figure provides a cross-linkage between records. This "indenture-data" is considered further in 11.1, post, and the situation regarding data linking together indid-names in 2.9.3., post.

4.2.3. WISHES OF THE INDIVID. These may be expressed in words or by behaviour, but must be additional to the wishes which would normally be imputed to the individual by other members of the society in which he lives.

4.2.4. PRIVACY NORMS OF SOCIETY. As attitudes towards morals, propriety and individual autonomy continue to vary throughout Western (computerised) societies, it is dangerous to take any one set of standards for granted. The sociological evidence is limited, and it is particularly hard to assess people's attitudes towards a privacy threat to which they have not yet been exposed. (5) If, however, we assume that some consensus can be found, this can then be taken as the one constant factor.

Responsibilities can be linked to each of the other three factors, and one objective of the model is to do this with some precision (see 2.7, post). But first, a means of classifying privacy-risk situations, and illustrating the information-chain events, is required. The next section proposes a nomenclature.

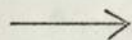
5. Interpretation in diagrams

Just as flow-charts are a useful tool of the systems analyst, so a visual representation of information-flow can assist in "privacy analysis".

The proposal is to show the information chain in diagram form, so that for any point in the chain one can deduce:

1. what restrictions apply to data flow
2. who is responsible for applying the restrictions
3. who is excluded from access by their application

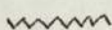
The symbols proposed are:



for the flow of an indid-datum



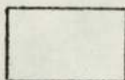
for controls implemented by people. (A control imposed specifically by one person on another will be shown directionally, thus $---->$)



for controls implemented by machines, or inflexible pre-determined procedures



for a person or set of persons



for a collection of data, or other impersonal source of data

EXAMPLE

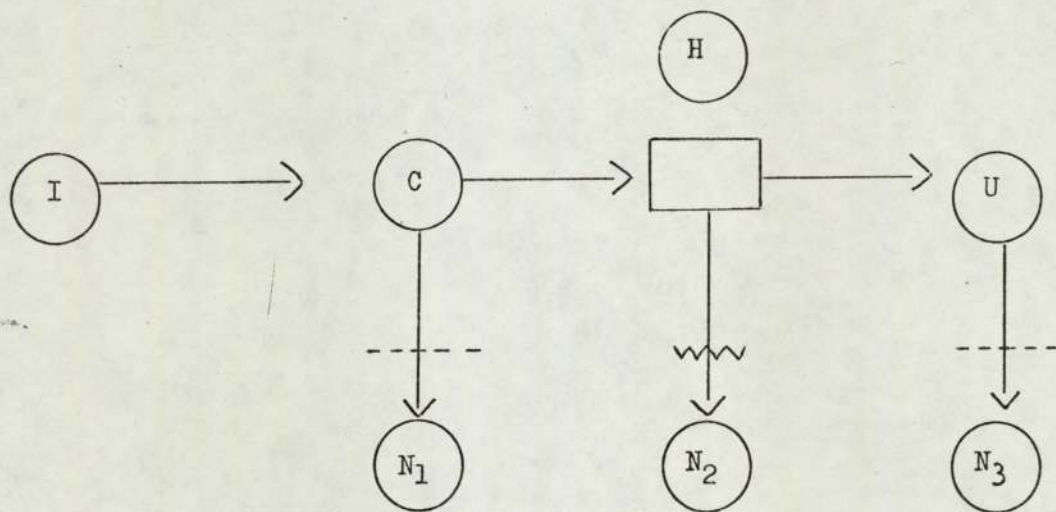


Figure (i) Indid-data

The figure shows the information chain for one indid-datum, eg., "indid I is bankrupt". The indid divulges the information to the collector C. I tells C that the information is given in confidence, so an obligation is created from C to I. C in effect undertakes not to pass the

information to N_1 - a large set of people excluded by the "in confidence" requirement.

C may also owe an obligation of confidence of a different kind to H, who runs the system. This will most probably be a general obligation (perhaps in the contract of employment) to treat all data as confidential, and will therefore be treated as "data-centred" confidence (see 12.3.1, post).

H depends on automatic controls to exclude access to the unauthorised population, N_2 . User U, being one of the people authorised to access the part of the database containing the indid-datum, can retrieve the data; but he also owes a general obligation of confidence to H.

One of the first aims of a privacy analysis should be to ensure that:

1. C, H and U all agree on the criteria by which populations are to be denied the data;
2. that U particularly, and C and H as necessary, are given a full appreciation of the circumstances and nature of the data, and the wishes of the indid, as defined earlier.
3. that in consequence, the proscribed populations N_1 , N_2 and N_3 are substantially the same, varying only in a few special instances where, for example, it may be proper for the collector to reveal data to person N_1 but not for the user to do so.

The diagram does not attempt to show:

1. anything of the circumstances which may surround acquisition of the indid-data. As suggested in 3.2.1. above, these may be

important. Furthermore, circumstances may change within the duration of the flow along the information-chain.

2. changes in the form of the information as discussed in 3.1. above.

The model can be refined to include these variables (see section 8), but for the moment the diagrams will be further developed with such variables assumed constant.

6. Context-data

Parallel with the flow of the indid-datum, we can plot the flow of associated, contextual data. For example, if indid I is bankrupt, it may be important to have an indication that this is someone's assessment of the situation, as proceedings are still pending. The diagram for the flow of this context-data will look like this:

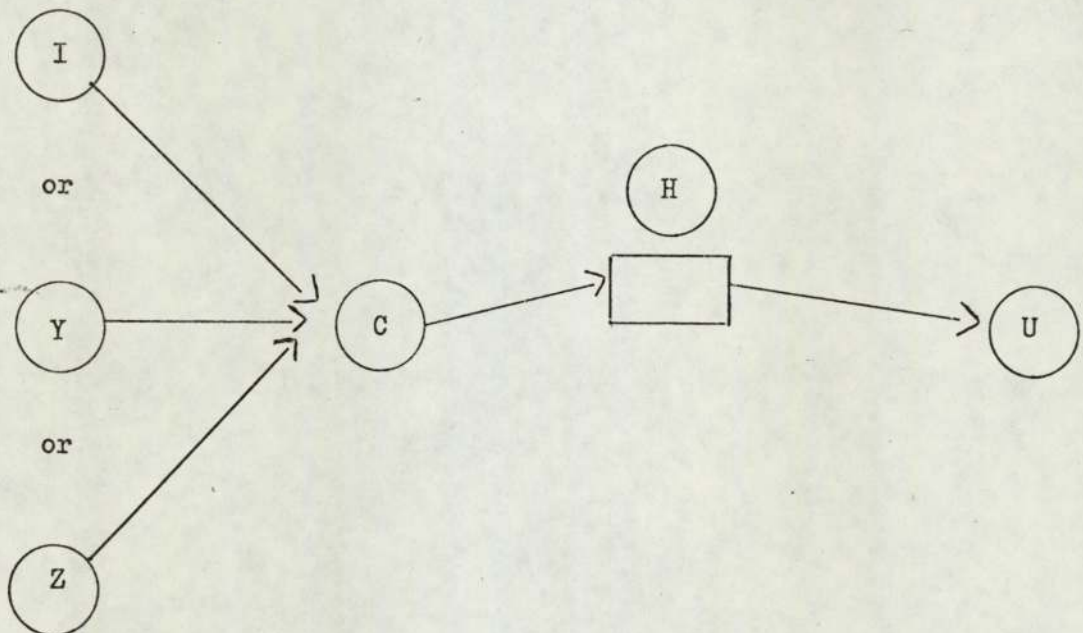


Figure (ii) Context-data

The pattern differs in that:

1. the context-data may come from various sources, i.e., may be observed whereas the indid-datum is divulged
2. there will usually be nothing private about the context-data itself: this will be assumed to be the case for the time being.

Sometimes it will be difficult to distinguish between context-data, and a new item of indid-data. However, context-data will usually take more the form of a hint or warning associated with the particular indid-datum. For example, if X is believed to be facing bankruptcy proceedings, there are two sources of doubt. Firstly, is the data from a reliable source? If not, an indication of doubt is certainly context-data. Secondly, what is the actual probability that X will end up in the bankruptcy court? It should be possible to convey this through the indid-data itself.

The distinction goes further than that sometimes drawn between "data" and "information". Context-data is needed not just to make the indid-data reasonably interpretable as information, but to enable judgments relating to privacy protection to be made responsibly and fairly.

7. Assignment of Responsibility

We now have two bases for discussing the responsibilities of I, C, H, and U. Using figure (i) we can consider responsibilities for ensuring the accuracy of the indid-datum, and the general pattern of responsibilities for restricting its dissemination. Using figure (ii), we can assess a related but possibly quite different set of responsibilities for each person in the model:

INDID. indid-datum: obviously a particular responsibility rests with the

indid, in divulging information, to make it accurate (see below); if confidentiality obligations are to be created by the indid, he must make them clear. context-data: if there are relevant circumstances which the indid expects, or ought to expect, that the collector will be unaware of, then the indid should point out the circumstances to the collector.

COLLECTOR. indid-datum: the collector must respect conditions of confidentiality set by the indid. He is also under an obligation to note and act on any aspects of the situation suggesting a need for extra confidentiality. If the datum is divulged, the indid should be told of the purpose for which it is being collected. context-data: any doubts about the reliability of the data, and conclusions drawn from the circumstances surrounding its collection, must be summarised and transmitted to the holder.

HOLDER. indid-datum: the holder must put into effect the procedures and controls necessary to respect the wishes of the indid and the collector. context-data: this must be passed on to the user, where appropriate.

USER. indid-datum: the user must respect privacy and confidentiality rights insofar as it appears to him that they apply, and should not assume that availability of the datum to him means that it should be available to anyone else. context-data: the user should take reasonable steps to establish whether any such data is applicable.

A responsibility rests on all four persons to make the information accurate. However, this can vary in legal terms:

INDID: information could be divulged under various conditions. For example: by virtue of a statutory requirement (census), on a form which

must be signed (rebate application), or in the course of an interview (market research). The strength of claim of an individual will normally be affected by the propriety of the way he divulges data. If he deliberately furnishes false information, he must weaken his claim to privacy with regard to that information. If he is negligent in the way he divulges information, he will have less moral standing in condemning negligence which leads to contravention of his privacy on the part of others. If, on the other hand, he gives accurate information and vouches that this is so, subsequent processors of the information must take care not to imply that he vouched for the accuracy of information which has subsequently been corrupted. Also, if the holder exercises a particular authority to require the provision of information, this will usually impose on him and his agents a stronger obligation to preserve confidentiality.

COLLECTOR: the collector could have a well-defined legal status, eg., doctor or census enumerator. However, in many cases, eg., local government officers, credit investigators, (6) no particular legislation applies. As at later stages in the information-chain, the deliberate and malicious alteration of the individual datum (and possibly the context-data) could give rise to liability in defamation. Similarly, there could be liability in negligence at any stage if financial loss to the ultimate user could be shown to result. (7)

HOLDER: in Younger Committee terms, the holder would be the "responsible person". In most situations, he will have some authority over the collector and user, as employer, principal, senior manager, etc. It is useful to distinguish two responsibilities:

1. vicarious responsibility for some of the procedures implemented by collectors and users;
2. general responsibility for the formulation of policy and the efficient running of the database.

USER: as the user is the destination of the datum in our chain, his responsibility is limited to careful use of the system, so that he retrieves as full and as accurate a picture as it can legitimately provide.

The assignment of responsibilities is discussed more fully in 12.3.1, post.

8. Conflicts

Ideally, responsibilities will be clearly agreed among the parties. The ideal may be approached in the majority of straightforward cases. However, every system for personal data must also expect to hit a fair number of awkward cases.

For example, the collector may owe confidentiality to both the indid and the holder, (ie., both indid-centred and data-centred). This causes no problems until one of them wishes to waive the obligation with respect to a certain datum. This then reflects a conflict between institutional and individual privacy rights, referred to earlier (2.3, ante).

"The public interest" may be raised by one of the parties as justifying a particular disclosure. Conflicts may also result from the partial view which every person necessarily forms of the total pattern of restrictions being applied: each has a different world-view. Each will want to be

assured that restrictions are being responsibly applied, but when such an assurance could itself involve privacy invasion we can only fall back on trust. Privacy cannot ultimately be disassociated from trust, as Fried has pointed out (8).

9. Refining the model

Our information chain moves through a fairly static landscape, and the model also fails to make allowances for the variations in meaning which result from changes in the form of the information.

9.1. time-variant factors. Privacy requirements will change if and when circumstances change, and the age and currency of information will also affect its privateness. Some general rules are proposed, as follows:-

9.1.1. where similar variations can be anticipated for all cases, responsibility rests with the holder directly. Standard procedures implemented throughout the system should provide adequate fairness, while avoiding the necessity for repeated decision-making. The duty of the holder is to see that such procedures are introduced and properly implemented.

An example would be, if records indicate nervous breakdown, or a minor insurance claim, then this will become less pertinent and less sensitive with the passing of time. Standard routines could therefore ensure that the data were erased, or accorded a different privacy status, at a given time.

9.1.2. Some variation will not, however, be easily anticipated. When these unexpected circumstances arise, anyone concerned with the running of the system should be obliged to act as the collector for the new context-data.

The holder's responsibility in this case is to minimise the fuss needed to make any alteration in the privacy protection for the individual concerned. At the same time, amendments should not be facilitated in the sense that they escape proper validation, nor should systems users or collectors be encouraged to be too positive in their search for relevant context-data.

Perhaps the points can be illustrated by a couple of hypothetical cases.

Suppose that Mrs. Y's maiden name was an unusual one, Z. She has not hitherto regarded this as being in the least bit private. However, a scandal blows up in the local press about another Z. Mrs. Y then becomes a good deal more sensitive about her maiden name.

Secondly, suppose that Mr. A has a mortgage with the B Building Society. He suddenly pays off the bulk of the debt with a single cheque. This is the result of a large pools win, which Mr. A. would prefer to keep quiet about. The state of his mortgage account therefore becomes an even more private matter than it is for the average customer.

It is tempting to treat such examples as being of academic interest only: the situation could arise only very exceptionally, reasonable people would not jump to conclusions, the repercussions of disclosure would be small. But the importance of privacy protection cannot be assessed solely in terms of the seriousness of the immediate repercussions if it fails, and still less by reference to the proportion of any given population for whom it proves to be individually relevant.

Privacy is also sometimes invoked as a means of avoiding unfair suspicion, as well as more ordinary embarrassments. In these circumstances, it tends to merge with more general issues of tact and discretion. Whether the claim to privacy is regarded as legitimate by others will depend not only on the privacy norms they accept, but their assessment of the probability or reasonableness of suspicions being aroused by the disclosure of the information. The individual faces a further obstacle, in that explicit requests for privacy may only draw unwanted attention to the situation: merely being in a position to need to make such a request may itself be a source of resentment.

All this suggests a requirement for careful reactions on the part of anyone who becomes aware of circumstances having a bearing on the privacy of individual data. The one thing that should not happen is that the responsibility for altering the context-data should be automatically seen as someone else's. Systems tend to encourage such an attitude. The solution is likely to involve having an office which is easily contactable, and always willing to accept responsibility for dealing with the matter. The holder would assume vicarious responsibility for its decisions.

9.2. changes in the forms of information. Without getting into the realms of philosophy, or the contemporary folk wisdom of Marshall McLuhan, it is enough to observe that the medium may matter at least as much as the message. A telephone call does not carry the weight of a document, and documents vary from teleprinter output to certificates or pound notes. Also, there are gradations in the certainty of information (hence the frequent recourse to "alleged", "believed" and so on in news reports), and some statements mean more than they seem to mean ("helping police with inquiries"). The law distinguishes hard and soft copy, in evidence, and recognises that innuendo may commonly be read into certain phrases.

The information-chain model is weak in this respect. As information moves along the chain, it changes. Like a commodity dispatched via air, rail and sea, it tends to turn up in different containers at different points, all the while showing the effects of the journey.

Since, by definition, the meaning of the information remains substantially the same, the privacy implications change only in degree. In this special sense, we can argue that the form of the information alters its sensitivity. For example, let us suppose that an intrusive information-chain proceeds as follows: (1) Mr. C is asked "how would you vote in a General Election?" and he replies "Labour". (2) This finds its way into a computer file under the coding: "political sympathy = Socialist". (3) Someone writes a report about C, and, having consulted the file, writes: "he has left-wing tendencies". Assuming that Mr. C found out what was going on, he would probably object more to this written report than to an equivalent remark over the telephone: equally, he would still object to both communications in principle.

The rule to be deduced is: never transfer an indid-datum from a medium carrying low authority (probably of low-definition and transient - "cool" in the McLuhan sense) to one of higher authority without ensuring that any implied increase in authority or veracity will be negated when the datum is next accessed.

This could mean either adding to the context-data, or altering the indid-datum in some way to introduce an element of uncertainty. The second option must be treated with care. Reverting to McLuhan again, by deliberately reducing the definiteness of a statement we may be in effect inviting subsequent users to clothe it with their own prejudices. (9)

9.3. data describing two indids. The previous section has outlined some dangers in thinking of an "indid-datum". This has been assumed to be of the form "identifier-descriptor". (10) However, files often indicate relationships between indids; for example, parent-child, employer-employee or doctor-patient. The form such linkages take within the database may be quite complex, but for present purposes, the database is simply a black box, capable of accepting and outputting the statement of the relationship.

The statements are troublesome because, although they can always be reversed without much change in meaning ("F is the father of S", "S is the son of F"), we have (as indicated in 3.1, above) to consider two different statements so far as privacy protection is concerned. For example, if F is respectable and S is notorious, S may be happy to broadcast the fact of his relationship but F may not.

Two different versions of the data have therefore to be recognised for privacy purposes.

10. Conclusions

Clearly no operational system is ever going to be able to offer privacy protection which allows for all the factors mentioned. However, the identification of such factors makes it possible to arrive at general conclusions concerning privacy-risk situations, and to design solutions which take cognizance of as many factors as possible. This objective is discussed further in Part III of this thesis.

CHAPTER 3
LEGAL SURVEY

1. Introduction

Discussing the "law of privacy" in the context of computers is rather like defining the edges of a hole. There is no legal recognition of a person's right to privacy. Certain remedies, offences, and requirements in legal proceedings act with the effect of protecting privacy, and so form the boundaries of the hole. These aspects of the law are reviewed in this chapter.

Since any further development of the protection of privacy would need to be rooted in existing legal principles, two areas of law are discussed primarily as sources of ideas capable of extension. These are Confidence and Defamation.

Broad studies of privacy in English law have been prepared for the Younger Committee, (1) and by Justice. (2) Analysis of the legal position relating more specifically to computers has been provided by Mallett (3) and Tapper. (4)

A final section of this chapter is devoted to problems of securing evidence when computer-stored information is involved.

The order of sections is therefore:-

2. Remedies in which privacy can be an incidental element
3. Criminal offences
4. Confidence
5. Defamation
6. Computer data as evidence

2. Remedies in which privacy can be an incidental element

2.1. Trespass. If information is obtained by venturing onto private property, the intruder may coincidentally commit the tort of trespass to land or goods. The remedy has been extended to someone spying from a highway over the defendant's land. (a) However, the remedy is available only to the person in possession of the land, who is not necessarily the indid.

A private nuisance may also derive from watching and besetting premises. (b)

2.2. Copyright. Copyright exists in any original literary work, even if unpublished. (c) As with confidential information, "originality" may derive from the organisation or analysis of freely available information, (d) so that a holder might claim copyright in a complete data file. (e) For the indid, protection will depend on the (often fortuitous) eventuality that he has copyright in the particular form of information about him. (f)

(a) Hickman v Maisey [1900] 1 Q.B. 752

(b) Lyons v Wilkins [1899] 1 Ch. 255

(c) Copyright Act, 1956, s.2 (1)

(d) Leslie v J. Young & Sons [1894] A.C. 335; Cramp & Sons v Frank Smythson Ltd [1944] A.C. 329; Ladbroke (Football) Ltd v William Hill (Football) Ltd [1964] 1 All E.R. 465

(e) The Copyright Act defines literary work in terms of "written" material (s.48 (1)), so it is not clear whether non-eye-readable material is covered. The Banks Committee were doubtful on this point: "The British Patent System" Cmnd 4407, 1970, at para 472.

(f) Williams v Settle [1960] 1 W.L.R. 1072

2.3. Natural Justice. Natural justice requires that if a judicial or quasi-judicial decision is made about someone, he or she should be able to challenge any evidence likely to affect the decision. This can include erroneous information kept "on the record" by the local branch of a trade union, (g) or letters containing comments relating to professional competence. (h) However, the person accused cannot object to the acquisition or use of evidence on the ground that the means of obtaining it were intrusive. In Byrne v Kinematograph Renters Society Ltd, where the defendant's agents made several secret inspections of attendances at the plaintiff's cinema, Harman J commented: "It was said, in addition, that the plaintiff's privacy was invaded by the inspectors, and that this was some act of unlawfulness apart from trespass. I can only say that I do not appreciate this argument." (i)

The applicability of natural justice is in any event limited by the need for some kind of contractual relationship between the parties. The anomalies which result from this have been documented extensively by Professor Lloyd. (5)

In the particular case of unfair dismissal, (j) there has now been added the statutory provision of s.24 of the Industrial Relations, Act, (k) but

(g) Breen v A.E.U [1971] 2 Q.B. 175

(h) R v Architects Registration Tribunal, ex parte Jagger, [1945] 2 All E.R. 131

(i) Byrne v K.R.S. Ltd [1958] 2 All E.R. 579

(j) Ridge v Baldwin [1963] 2 All E.R. 66; Re Godden [1971] 3 All E.R.20; sometimes the loss of job is indirect, following expulsion from an association - Weinberger v Inglis [1919] A.C. 606, Edwards v S.O.G.A.T. [1970] 3 W.L.R. 713

(k) Industrial Relations Act, 1971, s.24 (6)

according to one of the first cases under this section, it is the outcome and not the procedure which must be fair. (m) If this rather unusual principle is accepted, the employee would appear to have no right to challenge what was on the record, at the time of the dismissal.

3. Criminal offences

Strict statutory requirements of secrecy apply to government employees, (n) and employees of the Post Office. (o) Inspectors of health and safety may also be under an express duty to keep commercial information secret, though the exact nature of the duty may be a bit vague. (p)

No legislation creates equivalent offences in respect of local government. An officer might commit an offence in some circumstances by selling information, but, as Professor Street has pointed out, (q) the

-
- (m) Earl v Slater & Wheeler (Airlyne) Ltd [1972] I.T.R. 387. The tribunal's jurisdiction was held to be "confined to deciding whether a dismissal was fair or unfair, not according to whether the procedure adopted was".
- (n) Principally the Official Secrets Act, 1911, s.2 (1). Also, in connection with government information, the Census Act, 1920, s.8, and the Public Records Act, 1958, s.5 (2). For a discussion of the impact of Official Secrets legislation on local government see D. Foulkes, "Local authorities and official secrets", Local Government Chronicle, 12th Oct 73, p.1080.
- (o) Post Office Act, 1955, ss.55-58; Post Office (Data Processing Service) Act, 1967 s.2, and the similar provision of s.65 of the 1969 Post Office Act; see also s.80 of the 1969 Act.
- (p) e.g., plans furnished to an inspector "... to be kept secret...", Alkali, etc., Works Regulation Act, 1906, s.12 (1)
- (q) H. Street, "the officer who gives away information", Local Government Chronicle, 22 June 1973 at p.647

penalties are really reserved for those who accept bribes or otherwise misuse their influence in order to alter decisions.

Other offences which might be committed in respect of personal information are: the theft of recording devices (computer tapes or discs, for example), or coded pulses of electricity;(r) conspiracy to commit a tort, or even some less than illegal act deemed to be contrary to the public interest;(s) and the preventive measures of the Justice of the Peace Act, 1361, might be applied in respect of a continuing threat to privacy. (t)

4. Confidence

4.1. General principles. As commercial enterprise has come to depend more and more on the exploitation of intellectual rather than physical property, confidence has increased in importance as a method of protecting information relating to business operations, and the early stages of inventions. The equitable remedy for breach of confidence has therefore been discussed at length in the courts, but almost entirely in the context of commercial disputes.

-
- (r) Theft Act, 1968, s.13; or possibly theft of "intangible property" (s.4 (1)), assuming that one can "deprive" someone of such a thing (s.6 (1)).
- (s) e.g., Shaw v D.P.P. [1962] A.C. 220; Knüller v D.P.P. [1962] 2 All E.R. 898
- (t) "A remarkable range of conduct is customarily dealt with within the scope of preventive justice. Much of it lies outside the bounds of the criminal law..." D. Williams, "Keeping the Peace", Hutchinson, 1967, p.90

A preliminary definition of the basis of confidence is proposed: if A passes information to B in the expectation that B will use the information in A's interest as much as his own, then there is a breach of confidence if B exploits the information without regard for A's interest. A is entitled to an injunction to restrain B from using or disseminating the information, or, if the harm has already been done, to damages. (u)

In the commercial cases, there is very often a contractual relationship between A and B, so that damages are more often awarded for the breach of an express or implied contractual term obliging B to respect confidence. (v)

In its early days, confidence was used more to protect individual's privacy rights. Two of the earliest cases concerned the unauthorised publication of private letters. (w) In 1849, the case of Prince Albert v Strange (x) widened the protection to include etchings made for private amusement by Queen Victoria and Prince Albert. In 1888, a lady who had contracted to have a personal portrait taken, established her right to

-
- (u) Lord Cairn's Act, 21 & 22 Vict. c.27 (1858). See e.g., Microtherm Electrical Co. v Percy [1957] R.P.C. 207, per Lord Evershed
- (v) Robb v Green [1895] 2 Q.B. 315, ("It is impossible to suppose that a master would have put a servant into a confidential position ... unless he thought that the servant would be bound to use good faith towards him" - Lord Esher, M.R., at p. 317): whereas an express term had been included in the contract in Stephenson, Jordan and Harrison Ltd v MacDonald and Evans [1952] R.P.C. 10; the obligation may continue after repudiation of the contract, Ackroyds (London) Ltd v Islington Plastics Ltd [1962] R.P.C. 97.
- (w) Pope v Curl [1741] 2 Atk. 342, 26 E.R. 608; Gee v Pritchard [1818] 2 Swan 402. Injunctions prohibiting publication were issued in both cases.

prevent sales of copies of the photograph to the general public. (y)

It was at this point that the development of a legal right to privacy was given considerable impetus in America, with the publication of "The Right to Privacy" by S.D. Warren and L.D. Brandeis in the Harvard Law Review. (z) Emphasizing the aspects of privacy rather than property protection in cases such as Prince Albert and Pollard, they laid the foundations for the evolution of privacy rights: for just over a decade, their ideas led to dissension in the New York State Courts, (a) and the situation, at least with regard to the commercial exploitation of a name or portrait, was eventually clarified by statute. (b) Both a common law right and numerous statutory rights are now recognised in America, and have been discussed extensively elsewhere. (6)

Also in the last century, a separate line of cases developed in which information of commercial value was misapplied, usually by ex-employees. In Yovatt v Wingard, (c) the defendant set up a business to compete with the plaintiff's, using veterinary recipes which he had learned while in the plaintiff's employ. In Morison v Moat, (d) Moat, the son of one of the partners in a venture to manufacture medicines, somehow obtained the formulae from his father and, some years after his father's death, set up a rival business. The sons of the other partner, who were legitimately

(y) Pollard v Photographic Company [1888] 40 Ch. D. 345

(z) (1890) 4 Harvard L.R. p.193

(a) e.g., Mackenzie v Soden Mineral Spring Co. (1891) 27 Abb N.C. 402, 18 N.Y.S. 240, (injunction granted): Roberson v Rochester Folding Box Co (1902) 171 N.Y. 538, 64 N.E. 442 (injunction denied)

(b) N.Y. Sess. Laws 1903, ch. 132, ss.1-2, (amended on 1921)

(c) (1820) 1 J.W. 394

(d) (1851) 9 Hare 241, 68 E.R. 492

carrying on the original business, succeeded in obtaining an injunction to halt Moat's activities. Although Moat junior had given no undertaking to the Morisons he could still be prevented from exploiting his father's breach of confidence in passing on the formulae. A similar point was argued in Prince Albert v Strange, where the defendant had bought the etchings from one Middleton Judge, believing them to have been acquired by honourable means. The principle that innocent acquisition does not defeat the equitable remedy has since been asserted by Swinfen Eady J. in Liquid Veneer Co. Ltd. v Scott: (e) "It is quite clear that the Court will in the exercise of its equitable jurisdiction restrain an abuse of confidence by injunction, and it is equally true that the obligation of not disclosing confidential information extends to those who have acquired their information at second hand from the persons to whom the information has been confidentially imparted".

In terms of the information-chain model, the obligation of confidence therefore extends along the chain regardless of the degree of appreciation of the circumstances by individuals in the chain. While this may seem reassuring for the indid, it makes a consistent approach to the different legal responsibilities of people in the chain rather difficult. The implications with regard to eg., the Younger recommendations for a new tort of disclosing information illegally obtained (f) are discussed in chapter 12.

Apart from the relationships between individuals, the courts have also had trouble identifying the information to be treated as confidential. It

(e) (1912) 29 R.P.C. 639 at p.642; see also: Nicrotherm Electrical Co.Ltd v Percy [1957] R.P.C. 207 (per Romer L.J.); Printers and Finishers Ltd v Holloway [1964] 3 All R.R. 731 (Gross, J. at p.737)

(f) Younger Committee Report para 632

does not have to be secret, or absolutely original: "... the confidential nature of the document is not dependent on whether the information it contains is available elsewhere, but, on the question of whether it contains useful information which has been compiled by the plaintiffs for a particular purpose..."(g)

This protection has been afforded for suggestions for improvements to existing products, even though a good deal of the information incorporated into the suggestion might already be publicly known - the "springboard" doctrine. (h) On the other hand, information acquired by employees will not be protected in either equity or contract if it amounts to a general appreciation of management methods, (i) or even the names and addresses of 16 sales representatives, (j) although more extensive lists

-
- (g) Suhner & Co. A.G. v Transradio Ltd. [1967] R.P.C. 329, per Plowman J. at p.333; also, in Saltman Engineering Co. Ltd v Campbell Engineering Co. Ltd. [1948] R.P.C. 203, Lord Greene M.R.: "... it is perfectly possible to have a confidential document, be it a formula, a plan, a sketch, or something of that kind, which is the result of work done by the maker upon materials which may be available for the use of anybody".
- (h) Terrapin Ltd v Builders Supply Co. (Hayes) Ltd. [1967] R.P.C. 375 (case actually heard in 1959) per Roxburgh J.; Seager v Copydex Ltd [1967] R.P.C. 349: "When the information is mixed, being partly public and partly private, then the recipient must take special care to use only the material which is in the public domain... He should not get a start over others by using the information which he received in confidence", Lord Denning M.R. at p.368. See also Coco v A.N.Clark [1969] R.P.C. 41, per Megarry J. at p.47
- (i) Stephenson Jordan and Harrison Ltd v MacDonald and Evans [1952] R.P.C.10
- (j) Baker v Gibbons [1972] 2 All E.R. 759

may be protected. (k)

The trouble with these lines of thinking is that they stress the commercial value of the information rather than its potential for embarrassing the plaintiff. So for example someone might create a file of credit ratings and secure an injunction to prevent its reproduction, by virtue of the "work factor" which had gone into the list. However, an individual wishing to prevent his particular rating being divulged would have to proceed on a quite different basis. He would have to trace the source of the data on which the rating was based - say his bank account (m) - and show that a breach of confidence had occurred. Only then could he proceed against the current holder of the information. Few people are likely to regard this cumbersome process as worth pursuing.

A limited number of cases have centred on personal information. In 1896, the compilers of a credit index tried unsuccessfully to invoke the

(k) Louis v Snellie (1895) 73 L.T. 226. Lindley L.J., while holding that lists of names were protected, added: "If the defendant happens to remember that there is an agent whose address he can find out from the ordinary directories, he is at liberty to do it." This is not an entirely satisfactory exception, since the employee might happen to have a good memory for names. More commonly, of course, the employer will impose a reasonable restraint on the employee's future activities in the same line of business - e.g. Lyddon v Thomas (1901) 17 T.L.R. 450; Fitch v Dewes [1921] 2 A.C. 158

(m) an implied contractual term of confidentiality between bank and client will usually be assumed, but the courts have been hesitant in allowing it much scope: Hardy v Veasey (1868) L.R. 3 Exch. 107; Tournier v National Provincial and Union Bank [1924] 1 K.B. 461

protection of confidentiality for their credit assessments on individuals. A salesman left a copy of the index with a Mr. Saunders, who objected to the entry describing himself; the book's comments on two other people then found their way to the indids concerned. Libel writs ensued, and the credit index company counterclaimed on the basis of Saunders' alleged breach of confidence. The counterclaim failed. This index contained a notice to the effect that the information should not be disclosed, but in the absence of any contract of sale, this was held to be ineffectual(n) The case does however suggest the kind of situation where special provision is needed, in order that confidentiality regarding indid-data is not used against the indid. Lindley L.J. commented: "It may be that an index of the kind is useful in trade; but anyone who puts into it statements concerning a person's credit does so at his peril, and may render himself liable to an action for libel". (o)

It would be consistent with the sentiment of this, though stretching its meaning, to regard selective leaks to indids as legitimate acts, the consequences of which the compiler also faced "at his peril". The idea of distinguishing "data-centred" confidentiality in this respect is explored further in chapter 12.

A similar situation from the point of view of wielding confidentiality against the indid occurred in a case reported in 1912, this time founded on an implied term of contract. Mrs. Hitchcock contracted with a detective agency (which advertised its service as being strictly secret) for her husband to be kept under surveillance. One of the detectives left the

(n) Saunders v Seyd & Kelly's Credit Index Co. Ltd (1896) 75 L.T. 193; but see Bradstreets Britain, Ltd v Mitchell [1933] 1 Ch. 190.

(o) Saunders, ante, at p.194

service of the agency, and told a friend who told the husband. The judge concluded: "Whether a warranty ought to be implied that the servants would not commit breaches of secrecy while they were still in the plaintiff's service I express no opinion, but I think it impossible to hold that the plaintiff warranted that her servants would not make improper disclosure after they had ceased to be in her employment". (p)

There was no reason, however, why the agency could not hold its ex-employees to secrecy with regard to data on clients, being part of the agency's commercial property, and therefore no reason why the agency could not give sweeping promises of secrecy to clients if it so wished, in the expectation that these would be treated as warranties or even conditions of a contract. One suspects that the judge's reluctance to recognise such a warranty stemmed more from distaste at its possible use against the indid, rather than from the absence of a possible legal basis for doing so.

More recently, confidentiality was invoked successfully by the Duchess of Argyll, to prevent publication of articles by her ex-husband about their marriage. Granting the injunction, Ungood-Thomas J. stated that marriage undoubtedly created obligations of confidence, going beyond any element of contract and surviving the marriage itself. Of the breakdown of the marriage he said: "... what it does is to undermine confidence for the future and not betray the confidences of the past". (q)

The case provides an interesting example of the rights of an indid where the information necessarily relates to two people: the Duchess in effect held a veto, even though the information related to her husband as

(p) Easton v Hitchcock [1912] 1 K.B. 535, (Hamilton, J. at p.537)

(q) Duchess of Argyll v Duke of Argyll [1967] Ch. D. 302, at p.332

much as herself. (r) Also, the information was observed, rather than created or divulged.

Finally, more political consideration surrounded the injunction sought by Mr. Maurice Fraser against the "Sunday Times". Mr. Fraser was bound by an express contractual term to keep secret all reports he prepared for the Greek government. However, the Court of Appeal did not regard this as imposing any reciprocal obligation on the Greek government to treat information from or about Mr. Fraser as confidential.(s) Lord Denning stated emphatically that injunctions ought never to inhibit the publication of matters of public importance, and it is to this particular topic of the "public interest" that we now turn.

4.2. Public Interest. The doctrine with regard to confidence was summarised by Wood V.C. more than a century ago: "... there is no confidence as to the disclosure of iniquity. You cannot make me the confidant of a crime or a fraud." (t)

If indeed a crime is involved, then the issue is clear-cut. More often, however, the evidence is inconclusive or the act is not yet committed. In Gartside v Outram, a woolbroker's sales clerk told a customer about falsified notes of sale; in Initial Services v Putterill (u) an employee of

(r) A similar "AND" rather than "OR" requirement exists with regard to joint ownership of copyright. Cescinsky v George Routledge & Sons Ltd [1916] 2 K.B. 325

(s) Fraser v Evans [1969] 1 All E.R. 8

(t) Gartside v Outram (1856) 26 L.J. Rep 113, at 114

(u) [1967] 3 All E.R. 145

a laundry told the "Daily Mail" about agreement among laundries to raise prices and attribute this, unjustifiably, to S.E.T.; and in Hubbard v Vosper(v) the defendant was the author of a book alleging dubious practices on the part of the Scientology organisation. The arguments for refusing to grant injunctions restraining publication in any of these cases follow three separate strands:-

- (i) the doctrine that someone seeking an equitable remedy should come to the court with "clean hands"; (w)
- (ii) that the public interest requires that individuals should be able to speak frankly about activities which have possible anti-social implications. This consideration was uppermost in Lord Denning's mind in Hubbard when he held that: "... there is good ground for thinking that these courses contain such dangerous materials that it is in the public interest that it should be made known." (x)
- (iii) finally, the terms of a contract which seem to impose confidentiality may be regarded as contrary to the public interest.(y) The view of the courts on this point has tended to be pragmatic rather than moralistic, and hence not censorious of dubious means to commendable ends: equally, though, they will not go as far as seeing an

(v) [1972] 1 All E.R. 1023

(w) The plaintiff does not have to be absolutely virtuous, only reasonably so - Argyll v Argyll [1967] Ch. D. 302 at p.331 (per Ungood-Thomas J.)

(x) [1972] 1 All E.R. at p.1029. Megaw L.J., however, emphasized reason
(i) - see *ibid* p.1033

(y) For a general review of public policy and contract law, see J. Shand, "Unblinking the Unruly Horse: Public Policy in the Law of Contract", 30 C.L.J. 144-167 (1972 Vol. A)

obligation to resort to illegal or irregular action where circumstances would seem to call for it. (z) The difficulties of applying this doctrine were well illustrated in Howard v Odhams Press Ltd (a). The plaintiff had worked on crossword competitions for various newspapers, including the defendant's: however, he was discovered subsequently to be exploiting this background in order to secure prizes in the competitions. Howard made a statement to the defendants, but a condition of this was that nothing in the statement relating to another newspaper (the "Daily Express") should be communicated to that party. The Court of Appeal held that the agreement was contrary to public policy, and therefore void. Greer L.J. recognised that the agreement might well have protected the public interest insofar as it prevented further frauds, (b) but in this case the means used could not be countenanced or justified.

5. Defamation

5.1. In view of the information-chain model (ante, chapter 2), the chain may be broken if a person or a system receives the information and distorts it in some way. The distortion can be by a deliberate act of asserting

(z) P. Winfield, "Public Policy in the English Common Law", (1928) 42 Harvard L.R. 76; however, in Buckoke v G.L.C. [1971] 1 Ch. 655, the Court of Appeal held an order to act unlawfully (viz. to drive through red traffic lights) to be lawful. Sachs L.J. candidly described it as "one of those compromise situations which are so typical of this country and the despair of those who regard law and logic as being one and the same thing" (p.670)

(a) [1938] 1 K.B.1.

(b) Ibid at p.22

something intended to be misleading and derogatory, in which case tortious liability may arise under a number of heads. Distortion can be initiated by person A, and propagated unwittingly by person B, in which case B's liability is difficult to assess. Or a distortion could arise in the course of automated data processing, a prospect which exercises systems designers, and which is sometimes discussed as part of the general topic of privacy. (7)

Yet this distortion makes it difficult to decide in what sense one can now talk about "private information". To the independent observer, it may appear to be private, while in fact being false, so that any expectation he may have that the individual will want to restrict dissemination of the information will be based on erroneous grounds. On the other hand, the means of obtaining the information might have been both unreliable and disrespectful of privacy (as, for example, if someone stole a magnetic tape and decoded its contents wrongly), so that defamation and invasion of privacy could be compounded.

Notwithstanding this difficulty of finding a dividing line between defamatory and private information, the way that defamation has evolved as a remedy indicates ways in which privacy protection might also develop, in an information-rich society. For example, several of the defences which can be raised in actions for defamation provide protection for rights of free comment and expression, and clearly a similar conflict of interest can arise in respect of privacy (c). Defamation also centres on the interpretation of statements, in terms of what they were meant to convey and how they were in fact understood, and similar rules might be needed for deciding whether a

(c) The defences proposed in the 1969 Right of Privacy Bill (clause 3) have many similarities to defences in defamation

statement has in fact conveyed information which was subject to expectations of privacy.

Apart from defamation, false statements published with an intention to cause financial loss or other actual damage are actionable, (d) and a reputation which has a commercial value will be protected. (e) However, injury to feelings resulting from a loss of personal reputation is not a head of damage recognised by the courts. (f) It is undesirable that privacy protection should be based on any such criteria of quantifiable damage: otherwise, the privacy of organisations, relating to information of commercial value, will in effect be protected much more strongly than the privacy of the individual.

5.2. Privilege as a defence. With a few exceptions, (g) privilege derives from a social or moral obligation to communicate otherwise defamatory information. (h) Any inaccuracies giving rise to the defamation must be

-
- (d) Ratcliffe v Evans [1892] 2 Q.B. 524; see also Evans v Harries (1856) 1 H & N 251, 156 E.R. 1197; Balden v Shorter [1933] 1 Ch 427.
- (e) Finlay & Co. v N.V. Kwik Hoo Tong Handel Maatschappij (1929) 1 K.B.400; Groom v Crocker [1939] 1 K.B. 194
- (f) Addis v Gramophone Co. Ltd [1909] A.C. 488
- (g) e.g. publications issued by order of Parliament. Parliamentary Papers Act, 1840 s.1
- (h) Toogood v Spyring (1843) 1 C.M. & R. 181, 149 E.R. 1045, per Parke B at p.193; Pullman v Hill [1891] 1 Q.B. 524, per Lord Esher at p.528; Adam v Ward [1917] A.C. 309, per Lord Dunedin at p.323; Watt v Longsdon [1930] 1 K.B. 130, per Scrutton L.J. at p.142

the result of excusable error rather than malice. (i)

Under the head of duty to communicate, the courts have included: a solicitor protecting the interests of creditors by advising auctioneers of court action pending against a client of theirs; (j) a letter from the proprietor to a tied tenant of an inn, alleging that the beer was being watered, the letter being read aloud in the presence of secretarial staff; (k) and the circulation of a report, including derogatory references to an ex-secretary, among the committee of a Friendly Society. (m) A line of older cases derived from references written about domestic servants, the tone of which must be set against the different conditions of employment of the time. (n) While the common interest of old and new employer must be clear enough, others are more obscure: for example, in one case the duty of passing on allegations about a valet was described as that of "a host to his guest". (o)

It will not usually be sufficient that the defendant believed, however reasonably, that a duty to communicate existed: (p) there should also be a

-
- (i) Angel v H.H. Bushell & Co. [1968] 1 Q.B. 813
- (j) Baker v Carrick [1894] 1 Q.B. 838
- (k) Osborn v Thomas Boulter & Son [1930] 2 K.B. 226
- (m) Longdon-Griffiths v Smith and others [1951] 1 K.B. 295
- (n) see for example the reference quoted in Child v Affleck (1829) 9 B. & C. 403, 109 E.R. 150
- (o) Kay L.J. in Stuart v Bell [1891] 2 Q.B. 341, at p.360 but see strongly dissenting judgment of Lopes L.J. in that case
- (p) Hebditch v MacIlwaine [1894] 2 Q.B. 54 per Lord Esher at p.59; followed in Beach v Freeson [1971] 2 W.L.R. 805 (Lane J at p.813); but contra, on this point; Watt v Longsdon ref (h) at p.146

reciprocal duty or interest on the part of the person communicated to, to receive the information. (q)

Finally, the courts have always preferred to talk of privileged occasions, rather than privileged information. (r) In terms of the information-chain model, this means that privilege can be quite different at each junction in the chain. Several of the leading cases on privilege have involved only a later stage of a communication chain involving several people. (s)

It is submitted that if a right to privacy were created, such that people could be liable for communicating personal information when this was of a private nature, a similar defence of qualified immunity would be required. (t) Even in confidence cases, it might be preferable to develop a defence of privileged communication contrary to the confidence, rather than unduly stretching the concept of the public interest.

-
- (q) Hunt v Great Northern Railway Co. [1801] 2 Q.B. 189, per Lord Esher at p.191; Adam v Ward [1917] A.C. 309, per Lord Atkinson at p.334. The ratio of Toogood v Spyring ref (h) would seem to be that the plaintiff could be the recipient from the point of view of creating common interest, though not, of course, from the point of view of publication. See discussion of the anomaly, in White v J.F. Stone [1939] 3 All E.R. 507
- (r) "... the defence of qualified privilege is a defence for the individual who is sued, and not a defence for the publication": Lord Denning, in Egger v Viscount Chelmsford [1964] 3 All E.R. 406 at p.409
- (s) Stuart v Bell ref (o); Watt v Longsdon ref (h); Coxhead v Richards (1846) 2 C.B. 569, 135 E.R. 1069
- (t) This defence was provided for in the 1969 Right of Privacy Bill (clause 3 (e)), but not the earlier Bill of 1967.

One negative aspect of the comparison must be mentioned. In some cases, the number of people deemed to have an interest in receiving the communication has been enormous. (u) Where the class of people to whom disclosure is justified is more or less unlimited, it is more helpful to talk about disclosure in the public interest, than to confer a universal reciprocal interest".

Mention should also be made of the blacklist cases, which could acquire a new importance in the edp environment. In Macintosh v Dun, (v) a "Mercantile Agency" offered credit reports on a commercial basis. Clients would apply by means of a form, naming whoever they were considering for giving credit, and undertaking to use the information "in confidence and for our exclusive use and benefit in our business." Lord Macnaghten said of the agency: "... information such as that which they offer for sale may be obtained in many ways, not all of them deserving of commendation. It is only right that those who engage in such a business, touching so closely very dangerous ground, should take the consequences if they overstep the law".(w)

Privilege was denied, for these "communication made from motives of self-interest by persons who trade for profit in the characters of other people". (x)

-
- (u) Adam v Ward, ref (h); Hunt v Great Northern Railway, ref (q); but see De Buse v McCarthy [1942] 1 K.B. 157 (no privilege between council and ratepayers)
- (v) [1908] A.C. 390 (Privy Council appeal from Australian High Court)
- (w) Ibid at p.399. Compare the comments of Lindley L.J. in Saunders v Seyd & Kelly's Index, section 4.1., ref (n), ante
- (x) Ibid at p.399

However, where motives were more communal, it seemed that privilege could apply. In Barr v Musselburgh Merchants Association, (y) a Scottish case, the defendants were a non-profit making organisation who circulated a list of bad credit-risks to traders in the Musselburgh area. Their list was held to be privileged. In London Association for the Protection of Trade v Greenlands, (z) the appellants were a similar organisation of traders. However, the issue was confused by the fact that the secretary to the Association had secured the offending report from a third party, and the two individuals had originally been sued as joint tortfeasors: the outcome according to Lord Buckmaster, was "such disregard of the rules of procedure that extrication from the resulting tangle has been all but hopeless". (a)

None of these cases therefore provides very strong authority. As for computer-based systems, since the computer offers as a primary attraction the rapid retrieval of data from current files, a computer-based credit bureau is not going to pre-occupy itself with the kind of specially commissioned investigations discussed in the London Association case.

5.3. Publication. Another aspect of libel cases, which may come to have wider significance in the context of edp systems, concerns the innocent publication of defamatory statements. Typically, a library circulates a publication or a retailer sells one, and thereby becomes an unwitting party to the dissemination of the libel. The question then arises of whether the lack of awareness was the result of negligence.

(y) 1912 S.C. 174

(z) [1916] 2 A.C. 15

(a) Ibid at p.20

The holder of machine -coded data might find himself similarly in possession of libellous data, which was then output by the system to a user. Some of the arguments could again be applied to private rather than defamatory information.

An early case was Day v Bream, in which the porter of a coach office was held not liable for the libel contained in a consignment of handbills which passed through his hands, but which he had no opportunity of inspecting.

(b) Similarly, in Emmens v Pottle, (c) the defendants sold a copy of a journal containing a defamatory article. Lord Esher held that they were "Innocent disseminators of a thing which they were not bound to know was likely to contain a libel". (d) But here some element of a duty of care was implied, and a similarly restricted duty was thought applicable in another case a few years later, involving the loan of two journals by the British Museum. (e)

Subsequent cases have tended to require a stricter duty of care. In Vizetelly v Mudie's Select Library Ltd, (f) Emmens was criticised, (g) and damages against a library which had circulated a defamatory book were upheld. An additional factor in this case, however, was the printing of advertisements, seeking recall of the offending volumes, by the publishers. These the defendants had not seen. The jury concluded that they would have done so if they had exercised proper care in running the business.

(b) (1837) 2 M & Rob. 54, 174 E.R. 212

(c) (1885) 16 Q.B.D. 354

(d) Ibid at p.357

(e) Martin v Trustees of the British Museum (1894) 10 T.L.R. 338

(f) [1900] 2 Q.B. 170

(g) by Romer L.J., ibid at p.180

The jury in Bottomley v F.W. Woolworth & Co. Ltd, (h) similarly concluded that the failure to note the libellous context of magazines on sale amounted to negligence. But the judge held that there could be no liability in the absence of knowledge of the contents of particular magazines, and his decision was upheld on appeal. The jury's finding, that Woolworth's ought to have made random checks on the magazines (which were American remainders, coming in at the rate of about 50,000 per week) was described by Scrutton L.J. as "absurd and irrelevant". (i) His comments echo Lord Esher's in Emmens: "There was no evidence to justify a finding that there was in the nature of the magazine something which should have led the defendants to suppose that it contained a libel". (i)

Finally, in Sun Life Assurance Co. of Canada v W.H. Smith & Son, (j) the Court of Appeal reverted to a tougher line. The defendants had displayed posters advertising "grave disclosures" about the plaintiff's company. The posters were distributed by a rapid, routine process over which local employees had no control. There therefore arose a classic situation of duty and authority being found to reside in the wrong places: the local managers were held to be under a duty to vet the posters they used, but in practice all decisions about what was displayed were taken centrally. Scrutton L.J. now observed: "... the company as such has no knowledge: the knowledge of the company is only that of some of its servants or agents". (k) I.e., all individual knowledge should be imputed to

(h) (1932) 48 T.L.R. 521

(i) Ibid at p.521

(j) [1933] All E.R. 432

(k) Ibid at p.436

the company. Since the 1952 Defamation Act, the "offer of amends" defence deriving from innocent publication has similarly not been available to any publisher whose servant or agent "concerned with the contents of the publication" acts in a negligent way. (m)

5.4. Innuendo. According to the famous dictum of Lord Blackburn, there are no words so plain that they may not have different meanings in different circumstances. (n) The Courts have therefore pondered the meanings of "gone off", (o) "hocussing", (p) "blackleg", (q) and "bent", (r) among others. In the case of private personal information, the problems of innuendo are slightly different, in that the innuendo does not have to be derogatory. For example, a bank might give a favourable credit reference, phrased in such a way as to convey quite precise information to someone familiar with the bank's jargon, which nevertheless breached the privacy of the bank account. (s)

(m) Defamation Act, 1952, s.4 (5)

(n) Capital and Counties Bank v Henty (1882) 7 App. Cas. 741 at p.771

(o) Harrison v Thornborough (1714) 10 Mod 196, 88 E.R. 691

(p) Broome v Gosden (1845) 1 C.B. 728, 135 E.R. 728

(q) Barnett v Allen (1858) 3 H & N 376, 157 E.R. 516

(r) Allsop v Church of England Newspaper Ltd [1972] 2 W.L.R. 600

(s) A point taken up by the author with the "Access" credit card organisation, the Credit Manager of which wrote: "Cardholders are and remain in account relationship with the participating bank from which their card was issued and Midland Bank Access Department function as an entirely separate unit in a similar manner to a branch of the bank", (Letter, 23rd October 1972). The point not specifically denied in his reply was that the Access consortium obtained guidance as to credit ceiling suitability, in some form, from the customer's bank account.

Arguments that the ordinary man will tend to opt for a derogatory meaning if there is one (t) cannot therefore be transposed.

In the context of an information system, there should not be any doubt about the relation between indid and indid-data. However, if a person were alluded to in the record of another indid, innuendo relating to identity (u) might be important.

In both cases, scope exists for what might be termed "system innuendo". Once data has been made non-eye-readable it may be reinterpreted in many ways. The system or the people using it may develop codes of interpretation which are unfamiliar to the outside world, but which nevertheless facilitate the exchange of private information. (v) It should also be noted that certain kinds of innuendo can cease to exist in a computer, if all they comprise are one or two important characteristics of an unnamed person. (w)

(t) Lord Devlin, Lewis v Daily Telegraph Ltd [1964] A.C. 234 at p.277

(u) Chubb v Flannagan(1834) 6 Car & P 431

Fournet v Pearson (1897) 14 T.L.R. 82

(v) Thus requiring a test opposite to that proposed by Pollock C.B. in Hankinson v Bilby (1847) 16 M & W 442, 153 E.R. 1262, viz: "Words uttered must be construed in the sense which hearers of common and reasonable understanding would ascribe to them, even though particular individuals better informed on the matter alluded to might form a different judgment on the subject."

(w) as per J'Anson v Stuart (1787) 1 T.R. 748; or Newstead v London Express Newspapers Ltd [1940] 1 K.B. 377

6. Evidence

6.1. Introduction. To demonstrate that an invasion of privacy has occurred, the complainant must be able to show how the personal information about him got into the computer files. This presupposes that he can establish what that information is (or was, at some particular instant in time). This section examines the problems that would arise if actions for invasion of privacy were maintainable against data holders, (or if the liability arose earlier in the information chain, and the computer data was still needed in evidence).

6.2. Securing the production of evidence, and authenticating it.

6.2.1. Background. The first major conflict between the rules of evidence and dependence on automated records came in Myers v D.P.P., (a) a case which divided the House of Lords. Evidence was needed of cylinder block numbers, as recorded by a car engine manufacturer. Unfortunately for the prosecution, it emerged that the recording was systematic to a degree that no-one could be identified as having made the particular entries at issue, for storage in microfilm files. The evidence therefore remained hearsay. Their Lordships declined to make a "positive alteration" (b) in what was regarded as "settled law", (c) but the minority view was strongly put by Lord Pearce: "In my opinion, where the person, who from his own knowledge made business records, cannot be found, and where a business produces by some proper servant, who can speak with knowledge to the method and system

(a) [1964] 2 All E.R. 881

(b) Lord Morris of Borth-y-Cest at p.889

(c) Lord Reid at p.887

of record-keeping, its records reliably kept in the ordinary way of business, they should be admitted as prima facie evidence". (d)

In the following year, the Criminal Evidence Act made evidence of the Myers kind admissible. (e) However, in defining a "document" such as might be produced in court, the Act referred to "any device by means of which information is recorded or stored". (f) The Bar Association for Commerce, Finance and Industry drew attention to the ambiguity of this phrasing, which might cover a computer in toto as much as a particular tape. (g)

The position with regard to civil evidence was further revised by the Civil Evidence Act, 1968. This incorporates a better definition of "document", (h) but makes heavy weather of defining admissible computer output. A computer is defined as "any device for storing and processing information". (i) Under this definition one can include: an abacus, a television set, or an electric toaster, (j) or any of the following items

(d) Ibid at p.900

(e) Criminal Evidence Act, 1965 s.1 (1). The situation in civil proceedings was covered by s.1 (1) of the Evidence Act, 1938, (since replaced by s.4 of the Civil Evidence Act, 1968, as implemented in SI's 1969/1104 and 1970/18)

(f) Criminal Evidence Act, 1965 s.1 (4)

(g) Memorandum to the Lord Chancellor, "Computers and Discovery", (duplicated document, 6pp) 1967. See also New Law Jnl, 24 August 1967, p.917

(h) Section 10 (1) (c)

(i) Section 5 (6)

(j) The timer accepts data input and processes it according to the loop "has time been exceeded? no: repeat question, yes: eject toast." Tapper points out that a conventional filing cabinet might also fall within the definition: reference 4 at p.30

in a normal computer configuration: VDU, cpu, disc drive, tape drive, card reader, multiplexor or console. A catch-all definition might be thought desirable, but other sections such as 5(3) and 5(5) are then unnecessary. It is submitted that for evidence purposes a "computer" would be better defined in terms of a combination of devices assembled with a view to storing information with precision or longevity exceeding that of normal human memory, and to performing data-dependent logical operations on that information.

Other matters on which the section's coverage seems inadequate are:

- (i) 5(2)(a) and 5(5)(b). The document must be produced during a period when the computer was used for "activities regularly carried on"; and, picking one's way through the ambiguity of 5(5)(b) (reading "stored ... by" and not "supplied ... by"), it seems that batch processing temporarily or physically separate from the regular activities is envisaged. This is common enough practice. However, it is difficult to see why regularity is of the essence. (m) In a computer environment, it cannot be assumed that if an identical process has been applied to n data items without mishap, then item $n + 1$ must be dependable. This is because the computer very often goes further than the mere automation of records as instanced in Myers. For example, some quirk in a program may result in my account number triggering a routine which deducts 1% from my account. It is no consolation to me that no-one else's account number does this.

(m) a point discussed by Tapper, reference 4 at p.28

It is submitted that the solution will be to give the party challenging the computer output the following rights:-

- (a) to require production of program documentation, and, if necessary, of program dumps, for expert analysis: (k)
- (b) to demonstrate that anyone concerned with the processing of the data had a prima facie motive for falsifying it; the onus would then be on the other party to demonstrate that such falsification would not have been feasible

Equally the party adducing the evidence would need to demonstrate that human procedures in the operation of data processing (not just the mechanism of the computer s.5 (2) (c)), were supervised in accordance with good professional practice.

- (ii) It ought not to be sufficient that details of the origins of a document should be given by "a person occupying a responsible position in relation to the operation of the relevant device" (s.5 (4)). (n) The person should also be able to demonstrate professional skill in the appropriate field of computing.

-
- (k) the mechanism should be available against third parties who may be in a better position to supply this, such as software houses, or manufacturers (eg., in connection with microprograms). Proper protection of commercial secrets would need to be guaranteed.
 - (n) Details of this responsible person, along with notice of intention to introduce computer evidence, must be provided within 21 days of the hearing being set: R.S.C. Ord 38, r.21 (1) and r.24

(iii) The definition of a "document produced by a computer" is not adequate to cover cases where data is output through remote terminals. If someone interrogates a database, and perhaps takes hard-copy output via his terminal, some evidence is needed that the interrogation has been carried out competently. The user should be able to show familiarity with the interrogatory procedures, and, ideally, have done a confirmatory run on the same enquiry.

The questions remains, however: even if the court will accept a computer-generated document, can such a document be obtained by discovery or subpoena?

6.2.2. Discovery. The difficulties of obtaining discovery of computer data were outlined by the commercial Bar Association. (o) The difficulties are principally that (i) the document must exist, and (ii) it must be in the possession or power of the party to the action: this has been taken to mean sole possession or power. (p)

Assuming that a magnetic storage device could be regarded as a document for this purpose, common sense dictates that the court does not want to be presented with an uninterpretable iron oxide surface. But no precedent exists for requiring an eye-readable copy to be made, (and the situation

(o) reference (g) above, section 2

(p) Under R.S.C. Ord 31 r.14; Chantrey Martin v Martin [1953] 2 Q.B.286; also Kearsley v Philips (1883) 10 Q.B.D. 465

does not fall within the cases where production would be impracticable. (q))
 An additional practical difficulty lies in identifying the fields actually required, especially if it was not a current version which was required, but perhaps, a version of two weeks ago which could be obtained only from a grandfather tape or a security copy.

The litigant is also hampered by restrictions on what he may seek to establish in "fishing expeditions" - so that, if the other party denies possession, it is not permissible to probe further with interrogatories. (r)
 However, it is extremely difficult to draft legislation which relaxes procedures for obtaining evidence, without opening the door to fishing expeditions, as a series of cases on s.7 of the Bankers Books Evidence Act, 1879, has shown. (s)

6.2.3. Subpoena. A witness may be required to produce documents, or other physical evidence, under a writ of subpoena duces tecum, but once again it is doubtful whether this could be extended to compel him to produce an interpretative copy of machine-coded information. The problems would multiply if the data was encrypted, or part of "indenture-data" within the meaning of chapter 11, post.

-
- (q) Mortimer v M'Callan (1840) 6 M & W 57, 151 E.R. 320; Sayer v Glossop (1848) 2 Ex. 409, 154 E.R. 552; quaere, if a copy were produced, might it be inadmissible as not having originated during "activities regularly carried on"?
- (r) Hall v Truman, Hanbury & Co. (1885) 29 Ch. D. 307
- (s) R v Bono (1913) 29 L.T.R. 635; Waterhouse v Barker [1924] 2 K.B. 759; Williams v Summerfield (1972) 116 Sol.J. 413; and see D. Pollard "Not Goin' Fishin", New Law Jnl 6 July 1972 p.602

6.2.4. Authentication. (see also 4.3.2., post) Where a document indicates willingness to accept an obligation or responsibility, evidence may be needed not only of the origins of the document, but of some mark of acceptance entered on it which shows that the person wished to be bound by it. Usually this will be by signature. However, since signatures cannot be recorded (t) on edp systems, the question of vouching for information takes on a new dimension.

The kind of situations which may be envisaged are: (i) an applicant for rebate answers questions from a clerk, who keys the replies straight into an on-line file. The applicant signs a small form indicating that he has answered truthfully. Has he in any sense "signed" the computer-record? (ii) a doctor enters data about a patient into a database. The data proves to be erroneous. Can it be proved that the doctor entered the data, and vouched for its accuracy?

Two questions are therefore suggested:

- (i) does the signature have to constitute evidence of the acquiescence and identity of the person signing, or will any mark, whose origins can be linked with the signatory, suffice?
- (ii) can a signature precede, or otherwise be separate from, the information it authenticates?

Legal cases have centred mainly on wills, and requirements such as that of s.4 of the Statute of Frauds, 1677. The following discussion centres on

-
- (t) at least on current commercial systems. Digitising equipment for signature input is feasible and may well come into wider use

the authentication aspect only. It is submitted that similar issues could be of some importance in assigning responsibility following improper behaviour in the computer processing of information; (this is discussed more generally in chapter 11, post)

The early case of Schneider v Norris (u) shows the desire of the judges to construe requirements for a signature in a common-sense way. Norris has a standard printed memorandum of sale, incorporating his name. He entered his customer's name in his own hand-writing. Lord Ellenborough held: "the printed name thus recognised is a signature". Where the person has written his own name at some stage in the document, there is usually no difficulty:(v) however, the name must appear in a way which implies authorship, (w) and it is not sufficient to sign "the most affectionate of mothers", even if the context clearly identifies that particular mother. (x) If identification has to be made from handwriting alone, this too is insufficient. (y)

(u) (1814) 2 M & S 287, 105 E.R. 388

(v) Ogilvie v Foljambe (1817) 3 Mer. 53, 36 E.R. 21 ("Mr. Foljambe presents his compliments ... he will not trouble Mr. O. with any further discussion, but agree to the terms ..."): Morison v Turnour (1811) 18 Ves. Jun. 175, 34 E.R. 284; Propert v Parker (1830) 1 Russ & M 625, 39 E.R. 240; Bleakley v Smith (1840) 11 Sim 150, 59 E.R. 831; Lobb & Knight v Stanley (1884) 5 Q.B. 574; but the whole document must be alluded to; Caton v Caton (1867) L.R. 2 A.C. 127

(w) Stokes v Moore (1786) 1 Cox 219, 29 E.R. 1137

(x) Selby v Selby (1817) 2 Mer. 2, 36 E.R. 1

(y) Hawkins v Holmes (1721) 1 P. Wms 770, 24 E.R. 606; Calvert v Archbishop of Canterbury (1788) 2 Esp. 646, 170 E.R. 484

A signature may cover amendments to a document: "... words introduced into a paper signed by a party, or an alteration in it, may be considered as authenticated by a signature already on the paper, if it is plain that they were meant to be so authenticated." (z)

A stamp, (a) or a lithograph, (b) may be used instead of a written signature, provided that the signatory has authenticated its use. Signature may be effected by an agent, (c) even if he is agent for both parties. (d)

Finally, the contents may be in a non-permanent medium such as pencil.(e)

6.3. Evidence illegally obtained. An indirect protection of privacy might be afforded if evidence obtained by illegal means could not be adduced in a subsequent prosecution. However, this is not the case in England - partly, of course, because the intrusion will in any case rarely be illegal, but mainly because English Law as opposed to that of the U.S.A. (f) recognises no such general principle. The point was put succinctly by Lord Goddard: "... the test to be applied in considering whether evidence is

-
- (z) Pollock, C.B. in Bluck v Gompertz (1852) 7 Ex 862, 155 E.R. 1199
- (a) Bennett v Brumfitt (1867) L.R. 3 C.P. 28; Jenkins v Gainsford & Thring 3 Sw & Tr. 93, 164 E.R. 1208; Goodman v Eban 1954 1 All E.R. 763
- (b) Reg v Cowper (1890) 24 Q.B.D. 533 (per Lord Esher at 535, but contra, Fry L.J. at 536)
- (c) Evans v Hoare [1892] 1 Q.B. 593
- (d) Durrell v Evans (1862) 1 H. & C. 174, 158 E.R. 848
- (e) In the goods of R.A. Osborne (1909) 25 T.L.R. 519
- (f) L.B. Schwartz, "Excluding Evidence illegally obtained", 29 M.L.R. 635, (1966)

admissible is whether it is relevant to the matters in issue. If it is, it is admissible and the court is not concerned with how the evidence was obtained." (g)

The admission of prosecution evidence obtained by dubious means is entirely a matter for the judge's discretion. (h) The appeal court will rule on whether the discretion was exercised wisely. (i) A suspect is not entitled to privacy on police premises, whether or not he has been cautioned. (j)

6.4. Privilege and the production of evidence. If documents are privileged with regard to production in court proceedings, this creates for all practical purposes an area of privacy. As a general rule, privilege can only be relied on by the Crown, (k) spouses, (m) and someone using the services of the legal profession. (n) Otherwise, it is up to the discretion of the judge. The situation with regard to civil proceedings has been

-
- (g) Kuruma, son of Kaniu v The Queen [1955] A.C. 197 at 203 (P.C. appeal from Kenya); approved in King v The Queen [1969] 1 A.C. 304. See also Leggatt v Tollervey (1811) 14 East 302, 104 E.R. 617
- (h) Callis v Gunn [1964] 1 Q.B. 495, at 502
- (i) R v Payne [1963] 1 All E.R. 848; Reg v Stewart [1970] 1 W.L.R. 907; comments, obiter, by Lord Denning in Ghani v Jones [1970] 1 Q.B. 693 at 706
- (j) R v Mills [1962] 3 All E.R. 298, at 302; Reg v Maqsd Ali [1966] 1 Q.B. 688, at 702
- (k) Crown privilege has been sought for personal information in eg., Broome v Broome [1955] P.190, Conway v Rimmer [1968] 1 All E.R. 874.
- (m) As now defined by sections 14 and 16 of the Civil Evidence Act, 1968
- (n) the "legal profession" includes salaried legal advisers: Alfred Crompton Amusement Machines Ltd v Commissioners of Customs and Excise [1972] 2 All E.R. 353. See also reference (7) at para 27 which assumed this privilege to apply

examined by the Law Reform Committee, who regarded this reliance on discretion as a policy which had "in general worked satisfactorily". (8)

The Committee distinguished five grounds for privilege, of which all but self-incrimination will now be examined briefly:

6.4.1. privilege in aid of litigation. There need not actually be a case pending, but the communication must relate to matters needing the solicitor's advice or representation. (o) So far as a particular document is concerned, the general principle is "once privileged, always privileged". (p) However, if a copy of a privileged document is obtained, this ground of privilege does not prevent introduction of the copy as secondary evidence. (q)

In the case of Campbell, (r) it was held that a client's address would not be protected from disclosure, being "... a mere collateral fact, which the solicitor knows without anything like professional confidence." (s)

6.4.2. privilege in aid of settlement and reconciliation. Any exchange made with a view to averting litigation may be privileged. This arises

-
- (o) Jones v Great Central Railway [1910] A.C.4.
 - (p) Lindley L.J. in Calcraft v Guest [1898] 1 Q.B. 759
 - (q) Lloyd v Mostyn (1842) 10 M & W 478; Calcraft v Guest [1898] 1 Q.B. 759; a copy made in furtherance of litigation will however be privileged - Watson v Cammell Laird [1959] 2 All E.R. 756
 - (r) Ex parte Campbell, in re Cathcart, (1870) L.R. 5 Ch. 703
 - (s) Ibid at p.705, per James L.J.

mainly in connection with marriage breakdowns (t) and industrial disputes. (u)

6.4.3. privilege protection a confidential relationship. A very few statutory provisions survive with respect to husband and wife. (v)

Otherwise, the law recognises no privilege for professional advice which is neither legal advice nor advice given in furtherance of conciliation. Thus a psychiatrist may be subpoenaed to give evidence in divorce proceedings, (w) and a journalist may be compelled to disclose his source to a Tribunal of Inquiry. (x) The position of medical and spiritual advisers has been discussed by Nokes. (9)

The rules outlined so far are by no means mutually exclusive, and may be complemented by the rules of equitable confidence. In Ashburton v Pape, although privilege did not prohibit the production of secondary copies, an injunction preventing their use in breach of confidence was granted, this being extended, on appeal, to court proceedings. Swinfen Eady L.J. commented: "The fact ... that a document, whether original or not, is admissible in evidence is no answer to the demand of the lawful owner of confidential information to restrain it from being published or copied". (y) However, the exact ratio of this decision has been obscured by inconsistencies among the reports of it, to which attention has been drawn by Tapper. (10)

(t) Mole v Mole [1950] 2 All E.R. 328; Henley v Henley [1955] 1 All E.R. 590; Pais v Pais [1970] 3 W.L.R. 830

(u) Now expressly covered by s.146 (6) of the Industrial Relations Act, 1971. M & W Grazebrook v Wallens [1973] I.C.R. 256

(v) eg., in criminal proceedings, Evidence Amendment Act 1853 s.3

(w) Nuttall v Nuttall and Twyman (1964) 108 Sol. Jnl. 605

(x) Att.-Gen. v Mulholland [1963] 2 Q.B. 477

(y) Lord Ashburton v Pape [1913] 2 Ch. 469 at 477

6.4.4. Crown privilege. The ground of this privilege was traditionally that disclosure of facts inimical to the interests of the State ought not to be compelled. However, it has not always been easy to determine where the interests of the State lie. Until quite recently, the courts were content to leave the decision to the minister concerned, regarding any questioning of his judgment as an exceptional recourse. (z) For twenty years or so following Duncan v Cammell, Laird & Co. (c) the ruling by the House of Lords that a minister's ruling should be final prevailed. Then in Conway v Rimmer, (b) their Lordships expressed concern at the attempted use of privilege to withhold reports on a probationary police constable. For varying reasons, (c) and with varying opinions as to whether Duncan was actually being over-ruled, (d) it was held that a judge might in some circumstances order production of the document so that he could weigh up the public interest for himself.

One argument in Conway caused it to be cited in subsequent cases: this

-
- (z) " ... perhaps cases might arise where the matter would be so clear that the Judge might well ask for it, (ie., the document) in spite of some official scruples as to producing it, but this must be considered rather as an extreme case." Pollock C.B. in Beatson v Skene (1860) 5 B & N 838 at 854; 157 E.R. 1415
- (a) [1942] A.C. 624
- (b) [1968] 1 All E.R. 874. See: H.W.R. Wade, 84 L.Q.R. 171
- (c) eg., inconsistencies in comparison with nationalised industries (Lord Reid, *ibid* 880); exigencies of war-time security in 1942 (Lord Pearce, *ibid* 908)
- (d) eg., Lord Reid distinguishes Duncan, but Lord Morris refers to the desirability of exercising the House's freedom to depart from precedent.

concerned the need to ensure candour in official communications. Views on this point had again varied, (e) but soon afterwards Conway was taken by Lord Parker as authority for stating that, where a duty to report existed, " ... it was said by their Lordships that it is difficult to think that anybody whose duty it is to make a fair and honest report will not do so even though no claim for absolute privilege is made". (f)

Thus Conway has been construed as laying down a doctrine opposite to that of the early authorities. (g)

A separate basis for protection has always existed with regard to information from informers, but with the advent of quasi-judicial bodies such as the Gaming Board, the House of Lords has gone back to first principles in preference to classifying types and sources of information. (h) Each situation must, it seems, be reviewed in terms of the balance between public interest and the rights of the litigant seeking to produce evidence: furthermore, " ... 'Crown privilege' is a misnomer", (i) "There is no

- (e) eg., report too routine to merit protection (Lord Reid, *ibid* 888): prospect of indid-inspection might even encourage candour (Lord Morris at 891); government should enjoy no better protection than private anterprise (Lord Hodson at 904)
- (f) R v Lewes Justices [1971] 2 All E.R. 1126 at 1131. The nearest to this express view in Conway would seem to be Lord Hodson's references at [1968] 1 All E.R. 912
- (g) Smith v East India Co. (1841) 1 Ph. 50, per Lord Lyndhurst at 55; Hennessy v Wright (1888) 21 Q.B.D. 509, per Field J at 512
- (h) Rogers v Secretary of State for the Home Department [1972] 2 All E.R. 1057
- (i) *Ibid*, Lord Simon at p.1066

question of any privilege in the ordinary sense of the word". (j)

The Crown does, however, have a power conferred by statute to decline to reveal even that a document exists, (k) and in practical terms this can be a more potent weapon than any privilege.

Although no ministerial claims to privilege were made, similar arguments about disclosure and the public interest arose in Norwich Pharmacal Co. v Commissioners of Customs and Excise. (m) The defendants refused to reveal the addresses of importers of a drug which was alleged to have infringed patent rights. Discovery was finally granted by the House of Lords. The "candour" argument was raised, and indeed accepted by the Court of Appeal; (n) in allowing discovery, the House of Lords stressed that addresses, not evidence, were being ascertained, (o) relating to people against whom there was strong prima facie evidence of wrongdoing. (p) There was also discussion of just how confidential the addresses were, since they would have been known to shippers and warehousemen: (q) however, it is

-
- (j) Ibid, Lord Reid at p.1060. See Lord Pearson, similarly, at p.1066. The demise of Crown privilege is examined by P. Jackson, "Privilege and the Public Interest", Local Government Chronicle, 19th October 1973 p.1108.
- (k) Crown Proceedings Act, 1947, s.28 (2)
- (m) [1973] 2 All E.R. 943
- (n) [1972] 3 All E.R. 813, per Lord Denning at 818. The first instance hearing is reported at [1972] 1 All E.R. 972
- (o) [1973] 2 All E.R. at p.969 (Lord Cross)
- (p) Ibid at p.950 (Lord Reid)
- (q) Ibid per Lord Cross at p.969, Viscount Dilhorne at p.961

submitted that the point is academic, since if the information had been accessible to the plaintiffs by this means they would hardly have undertaken the expense of two appeals.

The case provided an interesting obiter dictum from Viscount Dilhorne, reflecting the philosophy of the Younger Committee: referring to government departments, he said: "... information of a personal character obtained in the exercise of statutory powers, information of such a character that the giver of it would not expect it to be used for any purpose other than that for which it is given, or disclosed to any person not concerned with that purpose, is to be regarded as protected from disclosure, even though there is no statutory prohibition on its disclosure". (r)

(r) Ibid at p.961. The Younger Committee recommended that information given for one purpose ought not to be applied for another: para 592

CHAPTER 4TECHNICAL SURVEY1. Introduction

Much of the technical literature on privacy protection treats privacy as being closely related to security. Sometimes privacy is seen as security applied in a particular environment - for example, W.H. Ware has suggested that security problems not falling within the ambit of state security form part of "the privacy problem". (1) In some cases, it is assumed that high security must automatically enhance privacy protection. In the IBM manual for OS/MVT with Resource Security, (2) for example, the probability that "invasions of privacy are imminent" in the public sector is given as a reason for installing protective software. Yet, although the manual quotes a distinctive definition of privacy ("The right of people to determine for themselves to whom, when, and to what extent information about them is made available"), (3) the manual is devoted entirely to security. Resource Security has not been designed with the indid's right to control information flow in mind.

A clearer distinction is established in the NCC review of computer security. Early on, we are told: "privacy ... is outside the scope of this report". (4) The report gives as one reason for excluding privacy the fact that many instances of privacy invasion, although associated with computers, have turned out not to derive from misuse of the computer. While this is true, much the same point could be made about allegations of breaches of security. However, the NCC report states its terms of reference plainly.

In contrast, a number of underlying assumptions have usually been made in many discussions of security/privacy. These include:

- (i) that two classes of people can be identified - viz, "authorised" and "unauthorised" users of the system. Where selective access control is envisaged, the pattern may be refined to link authorised users with particular sets of data. There is usually little or no discussion of who exercises the authority in question, or of the criteria by which access should be allocated. This is seen as a non-computer problem: but in many working environments the computer system will itself be a determinant of the distribution of authority, so that a lot of the assumptions built into it by its designers may eventually be self-fulfilling.
- (ii) deriving from the first assumption, there is a further assumption that the system should produce only two responses - access, or no access.
- (iii) the unauthorised user is assumed to have some ulterior motive toward the holder of the data (rather as someone trying to obtain state secrets is taken to do so from hostility towards the state). The situation of someone occupying a legitimate position within the holder-organisation and acting contrary to the indid's privacy interests (perhaps because of a misplaced sense of what is in the indid's best interest) is never considered.
- (iv) The holder-organisation is commonly taken to operate on a strictly hierarchical pattern, so that "levels" of security can be equated with levels of seniority.

Conclusions reached in the technical literature have therefore to be set against these assumptions.

2. General Principles

Certain general principles can be defined which do apply equally for both privacy and security.

2.1. Privacy protection must be provided as an integral part of the system, not as an optional extra tacked on for the "sensitive" market.

2.2. There should be the highest possible ratio of discrimination. If someone is entitled to see information, he should be able to do so easily. If not, it should be made extremely difficult.

2.3. Protection should be cost-effective. Whilst it is misleading to treat protection as built-on rather than built-in (rather like providing seatbelts instead of providing a strong chassis), the holder will usually have an idea of the expense of a system having no privacy protection at all. The difference in cost should be minimised.

2.4. Operation should be fail-safe. In the event of malfunction the system should clam up rather than allow unpredictable releases of information.

2.5. Superfluous sophistication should be avoided. Just as an expensive loudspeaker does not improve the output from a bad amplifier, so an elaborate procedure will fail to compensate for any inadequate ones on which it is dependent. To take another analogy, it is no use designing a complicated maze and then planting bushes which grow only four feet high.

2.6. Finally, any useful sets of proposals will consist of more than just a catalogue of what is desirable. A systems designer or manager can take note of a list of "oughts", but unless he has unlimited resources, he has to

choose among the measures available. Ideally, every such choice should be part of an overall strategy, in which the return from the estimated outlay forms only one factor.

3. Identification

Some of the problems of identifying devices and their users will be explored.

It is no use building in elaborate procedures for allocating access rights to users, if the system can be persuaded by user A that it is dealing with user B.

3.1. Terminal identification. It is straightforward for the central processor, in a typical dp configuration, to require devices to generate codes to identify themselves. So long as all the devices are subject to surveillance and communicate with the cpu by dedicated lines, security is simple.

The problems begin with requirements for flexibility in assigning different logical names to devices, and in using portable terminals such as the IBM 2721. The 2721 is designed to input data only, but more sophisticated portable terminals can be foreseen. One company already markets the modem element, little bigger than the telephone itself, at about £150. (5) Once the system will accept input from any telephone number, identification rests entirely with the device: there is no way of checking the source number of a telephone call, except by calling back. (a)

(a) a P.O.C. representative at Datafair 73 confirmed that subscribers could not test the source of calls on the switched network.

The use of a separate telephone link to the computer operator may help, as Babcock has pointed out. (6) The gain is real only if the line is used by the operator to check the user's whereabouts by ringing him back, or if the operator's number is a closely guarded secret. In either event, the procedure for logging in gets cumbersome, and some of the appeal of entering/retrieving data via any 'phone disappears. An identification signal from the device itself may be preferred. In the case of the 2721, three identification characters are used, offering little security. (7) However, telephone links can be protected by a "black box" between the terminal and the telephone system, which generates the required telephone and a password at the touch of a button: both of these therefore remain unknown to users. (8)

3.2. User identification. Usually, positive identification of the user is required. But brief mention should be made of circumstances in which non-identification of the user might be needed to protect privacy. Suppose that information services were to be provided via cables (perhaps installed primarily for TV) to people's homes. They should be free to make enquiries of the system in anonymity, the only exception being for quantitative information required for assessing service charges.

Turning to positive identification, this can be physical or logical.

3.2.1. Physical. The physical characteristics which are the most likely contenders for practical use are hand geometry, fingerprints and voiceprints. Other unique characteristics exist, but the use of, say, dental patterns would take security into new realms of incongruousness!

With any device, there must be a trade-off between the discriminatory power available, and the cost. Discrimination can be positive or negative;

that is, if there are two classes of people, authorised and unauthorised, the device can err either by allowing access to an unauthorised person, or by excluding someone who is authorised. The first bias threatens the integrity of the system. The second could cause offence and annoyance. The best devices therefore select and measure those parameters which show the greatest variation between individuals. Since many characteristics follow a normal distribution (eg., hand dimensions), there are theoretical advantages in measuring two different characteristics with a low or negative correlation. However, this threatens to make the authentication process longer and therefore less acceptable to users.

It is important to distinguish between devices which re-measure the characteristics at each access time, and those using a recorded version - eg., an actual fingerprint - carried by the user. The second option offers few advantages over a badge system, unless it is envisaged that frequent checks will be made, whereby card-holders provide a fresh fingerprint to be compared with the card's version. No system capable of measuring and analysing fingerprints or voiceprints anew at each access time is known to the author, although research is proceeding into both possibilities. (9)

An operational system based on hand geometry patterns (measured in situ) is currently marketed by the Identification Corporation of New Jersey and evaluation has shown that if the dimensions are measured to within 1mm, the error rate is within 0.1%. (10)

Since any device must reduce the characteristics to a bit-stream for the cpu to recognise, it becomes particularly important to secure the lines between the device and the computer. Otherwise a few interceptions of the codings will make the elaborate equipment required in order to generate them completely redundant.

3.2.2. Logical. Logical discrimination depends upon the improbability of an outsider guessing a data sequence or procedure known only to the user and the machine. Clearly both parties must keep their secrets well. In the case of the user, whose memory is normally less robotic than the machine's, the need is for something short and easy to remember; once the details have to be kept in hard copy, the secrecy problems multiply. In the case of the machine, all codings must be kept in a protected store, and processed by the cpu for a minimal period of time.

The user may be helped by a portable memory that is not eye-readable. Commonly, this will comprise a security badge with magnetic codings on it. Badges of this kind are used in the IBM computer-controlled office security system, (11) and in the 2984 cash issuing terminal. Such badges may be stolen, and may be copied by not unduly complicated techniques. Hence Lloyd's Bank have implemented their 2984 network with the additional check of a 4 digit number, given to the customer in a sealed envelope. Up to four attempts can be made to enter the number, after which the machine swallows the card.

As with physical identification, a trade-off exists between the reliability of the discrimination made, and the cost and inconvenience of the procedures. In practice, the ceiling adopted for passwords which the user must memorise is about 8 characters. (a) The theoretical discrimination (ie., only one chance in several billion of a correct guess by outsiders, the exact figure depending on the character set used) will be reduced if multiple attempts are allowed, and if the password is devised to be mnemonic rather than strictly random.

(a) examples from IBM products are: A.A.S., 4 characters (+ IBM employee number); OS/MVT with Resource Security, 5 characters; (12) A.I.S., 5 characters; GIS, 8 characters; (13) IMS 8 characters; (14) CALL/360, 8 characters. (15)

The protection given by a password can be enhanced by changing it regularly. One method is to give users cards which state their current codeword and nothing else: such a card may be mislaid and yet give no inkling to the would-be intruder of whether it is a particular user's, or is still current. Alternatively, the user and the machine may carry out an operation on parameters known to both - such as the hour of the day or the month's sales figures. But, given the limited choice of such parameters available, the basis of the calculation will be difficult to keep secret for long.

Finally, it is important that when a password is entered, it should not be typed out or displayed at the terminal. Facilities such as print suppression (eg., on the 1050) or zero intensity display (on the 3270) are provided to this end. If printing cannot be inhibited, backspacing will help to obscure the characters. (16)

A promising technique, in a more long-term view, is the use of signature verification. This has the advantage of depending on a time-honoured method, with which is everyone is familiar. Techniques developed at the University of Connecticut rely on "reference signature vectors" - in fact, a set of average gradients measured along the signature. The divergences between the test signature and a reference signature are calculated and summed. Threshold levels for acceptable divergence have then to be set. Typically, these will only succeed in accepting and rejecting correctly in 70% of the cases. (17) Research at the National Physical Laboratory by P.J. Pobjee and others has concentrated on the dynamics of signatures, monitoring the time taken in forming the different parts of a signature. This use of the time-pattern rather than simply the geometry of a signature offers additional protection against

forgers, who may be adept at reproducing the appearance of a signature, but without following the time-sequence of its proper author. (18)

4. Selective Access Control

Having identified the user, the system must determine what kind of access that person is to be allowed. Usually this will involve consulting a matrix of greater or lesser complexity, in which permitted combinations of user, secondary store area, and type of operation are listed. Two general principles will always assist in keeping this checking process from becoming too cumbersome:

- (i) if data entries can be grouped in such a way that privacy requirements tend to be identical within a group, then larger store areas can be designated as requiring a particular mode of protection
- (ii) if procedures are designed to filter out "no access" cases as early as possible in processing, valuable machine time can be saved

However, considerable complexity may still derive from the matrix variables, discussed in the three subsections:

4.1. Users. The worst situation is where user requirements are very heterogeneous. If users can be grouped by type or status level, on the other hand, considerable simplification may be achieved.

4.2. Secondary store areas. The unit of data to be protected can vary from a single bit to several files - an enormous ratio of scale. The size of the data store (eg., number of characters) is no guide at all, since data may be more or less compressed, and more or less heterogeneous in its

implicit security content. However, a dividing line can be drawn in practice between systems protecting at file levels, and those protecting sub-division of files. The majority of systems actually implemented apply restrictions at file level.

4.3. Permitted operations. Systems, whether proposed or implemented, invariably distinguish READ and READ/WRITE capabilities. Further refinements of control may then relate to adding or deleting records, or treating certain data as executable.

In this respect it is important to note that privacy is concerned with intrusion per se. Security has a wider concern, in that an illegal WRITE or DELETE instruction can damage the database. However, privacy is invaded merely by a READ action. Clearly other illegal instructions might be used as a means to that end eg., issuing a WRITE instruction so as to alter a program which controls access.

4.4. Access control procedures. Control can be considered in three main stages:

- (i) has the user identified himself as being entitled to log in to the system at all? A table will be required for this identity check, indicating the acceptable combinations of time, terminal, user name, password etc.
- (ii) is the user's instruction (eg., READ filename) permissible? Here again, a table may be considered for each occasion that user X seeks to perform operation Y on file Z. This check is data-independent, ie., nothing depends on the actual value of the data held in file Z.

(iii) is the user entitled to execute his instruction on the data field, in the light of the value stored in that field, (possibly in another field in the record)? This is a data-dependent check. It could depend on the value of the data (eg., X may read all fields for salary <£2,000), or on the value of a field hereby.

In order to economise on system time, it is desirable to establish any "access denied" response as early as possible. For example, in a transaction-oriented system where the user may quote a filename as one of only a few parameters which he inputs, the system should check a table as in (ii) above before translating the command into object code and initiating the file access.

If the system allows programs to be developed and executed via a terminal, efficiency will similarly be aided if checks for illegal access requests can be made at, or just before, compile time. However, a skilled programmer might be able to circumvent such checks, for example by generating core or file addresses within the program. Where this possibility exists, the check needs to be made on the read instruction when it is actually implemented.

The problems of balancing efficiency and security have been analysed by Conway, Maxwell and Morgan, (19) and Friedman. (21) Conway et al point to the high overheads which can result from trying to build access tables for a random pattern of inquiries, and suggest that by careful planning of when the matrix is consulted during processing, reductions in these overheads can be achieved. They therefore propose that, during translation, a type (ii) table should eliminate users having no access rights to a file at all. Even if access were allowed, a call to a different

matrix function would be generated in the object code, and a data-dependent check would be carried out when the data was actually read. (20)

Friedman, on the other hand, argues more strongly for data-dependent checking, and the use of tags directly adjacent to data. He comments: "... every interval separating a protected field from its protection presents a slight but real opportunity for errors of reference to arise". (22) Such errors would presumably derive from careless programming rather than hardware faults, in which case one has to face a difficult yet telling question in deciding whether one system or another is more conducive of human mistakes in setting it up. Friedman cites a number of positive advantages for his approach, including the ease by which access can be adjusted to meet changing situations. The value of such tags in allowing flexible privacy controls is explored further in the discussion of a "privacy label" (post, 11.3.1.).

Turning now to two systems actually implemented:

4.4.1. the ADEPT-50 system. This system, as described by Weissman of SDC (23) is entirely data-independent. A "franchise" is extended to a user, or group of users. The set of users so defined may be with regard to a particular terminal, job or file. Users, terminals, jobs and files are all treated as "security objects", and each object can have defined for it not only a franchise but an "authority" (hierarchy of security jurisdictions) and a "category" (separate, discrete, security jurisdictions). "Jurisdiction" in this context has a vague meaning, but is a functional entity so far as the system is concerned. Given the authority for a user, for example, together with that for a terminal, the system can compare the level of seniority of the jurisdictions, and select the highest common level as

permissible. In the case of categories, the system simply computes the intersection of the sets. Such operations can be repeated for any combination of user, terminal, job and file, and from these operations it can automatically be determined whether a user is within the franchise for doing what he wants to do. In implementation, ADEPT-50 has 4 levels of authority and 16 types of category.

The beauty of the approach lies in being able to deduce the franchises automatically not only for each file access, but in the event of a new file being created from two originals. However, the system has been designed for the U.S. Department of Defense, and clearly has more to offer in the field of military security, where data is more easily classified according to the type and level of security it requires. Even so, one suspects that the actual assignment of 20 authority/category ratings to each security object, bearing in mind all the logical operations which will derive from these, may not be all that easy a task. The neatness of the model also disappears in practice when necessary restrictions are placed on its generality - for example, the franchise for a job can be only one user.

4.4.2. ASAP. This system embodies the ideas of the Cornell team of Conway, Maxwell and Morgan. They opt for checks at compile time, thus necessitating re-compilation of each job: this they claim "does not exact the penalty ... that might be expected". (24) The access is controlled down to field level, but there are only 8 different classes of access - all fields must fall within one of the eight. There is no hierarchy of classes. Data-dependent checks may be applied subsequently using a Boolean expression filed in the directory entry for each user. Thus access may still be denied if the data value is "male" or "3000" when the Boolean expression specifies "not male" or "<2000".

4.4.3. Hoffman's "formularies". This system is a part-implementation of a general model devised by L.J. Hoffman at Stanford University. (25) Hoffman's aim is to interpose a modular "formulary" between each user (or user program) and the database. Within each formulary, a CONTROL procedure makes whatever checks are necessary to authorise access.

The approach imposes a number of constraints on the way the system is used. Users are confined to logical addressing of data (not unusual), but must also communicate through special system procedures called TALK and ACCESS. These provide links between user and formulary, and user and data. The restrictions are balanced by the advantages of separating out the access control completely in one stage: the physical arrangement of the database can be changed, but security tied to the logical names, is unaffected. Equally, access patterns can be changed in a variety of ways by altering the formulary via which the user proceeds, and there is no effect on the database.

The tests applied by CONTROL cannot be all that far-reaching; Hoffman cites password protections, time of day, request for operator authorisation. But the main advantage seems to lie in the freedom to tailor the security procedure to each particular user. Since the formulary has to be set up by systems programmers (and, ideally, entered in special read-only memory), its flexibility in theory is not quite the same in practice: a way out of this may be to devise methods whereby users could transfer access authority from one to another. (a)

(a) At the end of his paper, Hoffman refers to studies of the feasibility of this being conducted by R.D. Russell. Some transferability is available to file owners in the system of D.K. Hsiao - ref (32).

Hoffman is wary of data-dependent checks, since any test based on actual data values may reveal a lot about one particular value - a point Hoffman was first to point out in an article written jointly with W.F. Miller. (26)

Hoffman states as an advantage of the formulary approach the facility with which the cost of access control (carried out entirely within the formulary) can be separated out from general systems costs. This is a useful byproduct but not in itself an incentive towards modular systems.

5. Control of executable data

The user of a system may be allowed widely varying degrees of freedom. On the one hand he may be confined to simple instructions of the form "read the record of indid X". Alternatively he may be able to write programs invoking files and peripherals. In either case the user-program (even if it is only one instruction) operates within an environment created by the system - so that the program sees a "user machine". (27) As the freedom of the user increases, so does the possibility that he may be able to alter the user machine in order to remove restrictions on his use of the system. Precautions must therefore be taken to ensure that certain programs stay unassailably in privileged mode: in this sense, it is more appropriate to talk about the constitution of the system rather than its architecture.

The simplest constitution is feudal. Serf-programs do the bidding of the aristocrat-program, which directs where the serfs reside, when they work, and what data they work on. System macros may have an intermediate level of authority, commensurate with their trustworthiness.

But more progressive constitutions allow the user programs to be stored, and called by other user programs; allow user extensions to be built onto system programs; and may also allow users to write low-level language instructions which are indistinguishable from those of the operating system itself. All these facilities aid the programmer who wants to thwart or overthrow the system.

5.1. General precautions. Three preliminary steps will help to protect the integrity of an operating system. These are:

- (i) assess which instructions need protection: (many cannot be misapplied, or their misapplication causes total breakdown)
- (ii) provide read-only protection for these instructions
- (iii) provide checks on the locations from which calls to these instructions originate

The third protection is particularly complicated, since it involves one part of the operating system monitoring another: and keeping track of addresses may be rendered more difficult by techniques of virtual storage and time-sharing.

5.2. Theory of control. Instructions needing particular attention are those which fetch and store data from the secondary store, and also the traps and other status code signals which pass control. Fetch and store instructions may be held by a separate file supervisor - as in Hoffman's ACCESS module - or may be an integral part of the operating system.

However, fast retrieval times from "secondary" storage and the development of sophisticated operating systems increasingly result in a blurring of the distinction between main and secondary storage. A general model of control mechanisms, not dependent on this hierarchy, is therefore needed.

B.W. Lampson has suggested a model of "capabilities" and "domains" for analysing transfers of control. (27) Capabilities are defined as system-protected names for any object (ie. component of the system) that a program may need to call. Domains occupy working space and hold varying groups of capabilities. By directing control to a domain, a program can therefore be made aware of more or less of the parts of the system. Furthermore, by going via a "switch" domain, programs can communicate in anonymity, ie., without revealing the source of a call.

5.3. Implementations.

5.3.1. ADEPT-50. The system executive has two parts: BASEX resides permanently in main store, while EXEX swaps in and out. BASEX maintains a record of the current status of each page of core, and pages of main memory can be both read and write protected. The security tables (SYSLOG) are loaded from cards onto a specially protected disc at start-up time.

Both core and drum pages are cleared to zero prior to each re-writing, (an option rated at maximal expense by the NCC guide (28)): the ADEPT-50 executive works in tandem with a standard IBM/360 operating system, the latter referring all interrupts likely to have security implications to BASEX.

A user can only enter the system via a LOGIN procedure, which checks the user/terminal franchise with SYSLOG. If the user requests a facility having to have privileged status, such as DEBUG, BASEX checks that the addresses requested lie in the user's program area. I/O requests are also monitored by BASEX. The system checks access to SYSLOG by requiring a special user-identification, and a check that the call is from one of a restricted class of its own executive-status programs. This further narrowing of executive privilege is in line with Weissman's advice, that especially with system breakdowns in mind, even executive programs should have the minimum privileges they really need. (29)

5.3.2. Multics. Parts of the executive are protected by hardware locks, preventing reading, execution or modification except in response to special interrupts. The supervisor has also been "compartmentalised", with a view to minimising the damage done if a user somehow succeeds in gaining illegal access. (30)

6. Techniques: meeting requirements

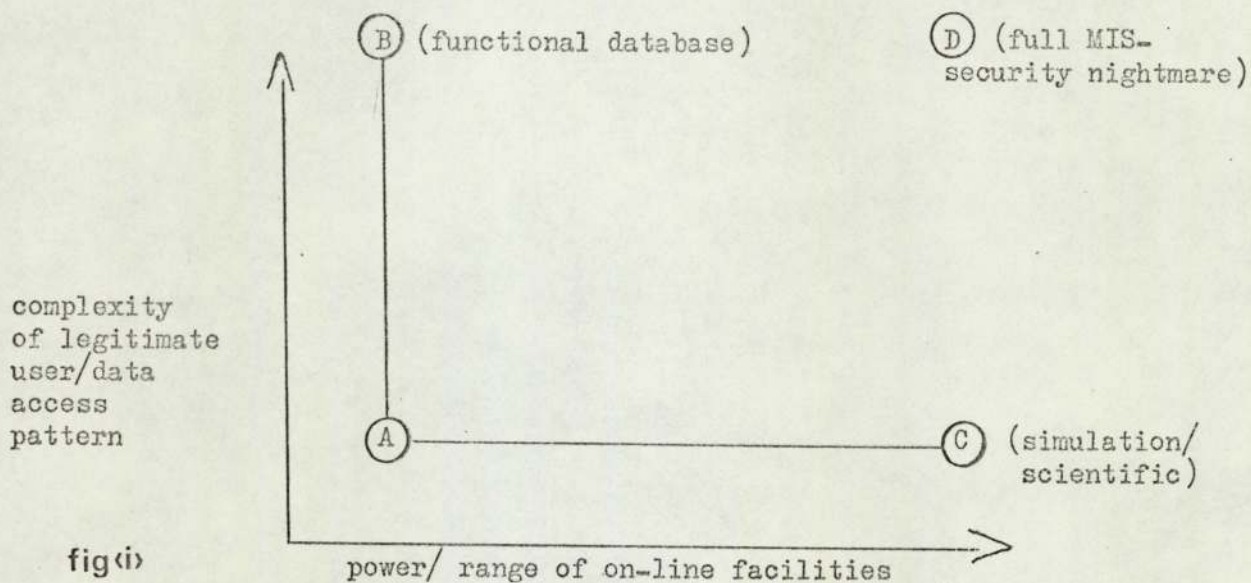


Figure (i) provides a simple model of security-sensitive environments.

System (A) has transaction users only. There are a limited number of users $\{U\}$ and a limited number of files $\{F\}$, so that the product $\{U\} \times \{F\}$ is small. The transaction programs either confine the user to entering keys or simple values (a CODASYL "Parametric" user (31)), or using a high-level query language (a second kind of parametric user, distinguished by CODASYL).

As we move from (A) to (B), the sets $\{U\}$ and $\{F\}$ increase in size. Consequently we need larger security matrices, and more time for any data-dependent tests in operation. However, this remains a simple if large database, with parametric users and quite probably not even facilities for writing on-line.

Moving from (A) to (C), we pass to another user type defined by CODASYL, viz, "program-oriented". He will require to be able to de-bug programs and re-organise files. Clearly he needs wider read and write access. However, he is assumed to be content to work with fairly limited data sets.

(D) represents the ultimate security problem, where users want a wide choice of files and programming facilities. The seriousness of the problem will still depend on the security need vis-a-vis the particular data/user group. It may be that security is only needed for a small set out of the total files, in which case security can centre on this "sub-database" falling lower down on figure (i)'s vertical scale.

Issues associated with each kind of system are:

6.1.1. Types (A), (B). The fact that a user is entitled to access information does not mean that the system should volunteer that information. The weakness of some inquiry systems is that they respond with blocks of data, which have to be whittled down iteratively: at each stage, the user narrows the search. (a) A discreet system will indicate that re-phrasing is necessary without displaying all the information.

Obviously the grouping of users and protected data sets should be simplified as much as possible. This calls not just for good current systems but anticipation of the ways in which the database and its use-patterns are likely to grow in the future.

6.1.2. Type (C). Where one user can determine the access rights of another (as in Hsiao's system (32)), the file "owner" acquires privileges intermediate to those of the system manager and the ordinary user. Supporting a hierarchy of privilege of this kind requires that the right scope and type of privilege is delegated to the middle-status user: (if the privilege is too circumscribed, he is unlikely to have effective control, vis-a-vis the ordinary user). Similar considerations arise with the "concentric ring" model, as proposed by Graham. (35)

(a) eg., the IBM manual for IQF under IMS (H20-1074-0) reads: "For example, a request for information on certain clerical personnel might elicit too large a response for a specific purpose. This request could then be immediately resubmitted with the request limited to a particular category" (at p.2.2.)

6.2. Finally, a brief mention should be made of the fourth kind of user defined by the CODASYL committee. He is the "data administrator" - arguably not a user as such - to whom the whole system is visible. Even in his case, it will be desirable to have his actions subjected to audit by devices which it is difficult to alter or deceive.

7. Identifying individuals in statistical searches

In type (C) and (D) systems, there may be a facility for asking questions of the form "how many people have attributes $a_i, a_z \dots a_j$?" Ostensibly this reveals nothing about any individual person. However, as Hoffman and Miller have pointed out (26) anyone knowing certain of the attributes $a_i, a_z \dots$ could devise searches designed to reveal the value of a_j .

Various techniques for preserving the anonymity of output from such searches have been proposed. (34) The situation is easiest where the data is specially collected, perhaps in a social survey. The range of data can be limited strictly to the needs of the survey, statistically distributed errors can be built into the source data, and the data itself will probably not be updated, so that its reliability as current information will come in question quite soon after collection.

However, in a local authority, the aim may be to use the data held in the administrative files as the basis for statistical analysis. If the authority wants such a facility on-line, the privacy problems are likely to be formidable. The desirability and practicability of creating such a facility are discussed in 5.4.1, post.

CHAPTER 5LOCAL GOVERNMENT SURVEY1. Introduction

Long before the reforms enacted in 1972, it was widely accepted that local government was working in unnecessarily diverse units, and that the division of functions between authorities lacked overall design in many respects. However, diagnoses and prescriptions varied. The Maud Committee, reporting in 1967, instanced the failure of councillors to delegate responsibilities to the paid officer, (1) and proposed that a "management board" of councillors should oversee council business (in effect acting as a local cabinet), with the Clerk of the Council as manager of all the professional staff. Abolition of legal restrictions on delegation and relaxation of the "ultra vires" rule were recommended.

Subsequently, the 1969 Royal Commission examined the whole issue of reform, and claimed to detect "a movement of opinion in favour of large authorities". (2) Accordingly England was to be divided into 58 unitary authorities, with a metropolitan/district structure in three of the conurbations. (a) The unitary concept was accepted by the government of the day, (3) but two metropolitan counties were added, (b) and education transferred to the upper-tier authority in the metropolitan areas.

The new administration of 1970 was less convinced by the Commission's arguments, and proposed a two-tier system, (4) since implemented in the 1972 Local Government Act. From April 1974, England will be divided into six

(a) Birmingham, Liverpool and Manchester

(b) West Yorkshire, South Hampshire

metropolitan counties, and 37 counties.

Shortly after the White Paper setting out the two-tier proposals, a study group was set up under the chairmanship of M.A. Bains, to look at the management structures which would be appropriate for the new system. Their report appeared in August 1972. (5) It contains echoes of the Maud Committee report, in urging more delegation to officers and the appointment of a chief executive officer. The concept of departments, each working under its own committee, now seems to be in decline: authorities now have much wider discretion as to whether they appoint committees at all, (c) and the Bains Committee commented: "As a general rule, we do not believe that it is necessary, or even desirable, for the committee and departmental structures to coincide." (para 5.74)

Adding to the uncertainty which this creates about the role of the elected member, demands have grown for the appointment of "ombudsmen" to investigate complaints on behalf of individual citizens. (6) The idea has been resisted by the C.C.A. (7) and others concerned to keep the "watchdog" role as the preserve of councillors. The Ombudsman apart, many difficulties arise as to what information the elected representatives are entitled to see, especially if they are in opposition. (8) The public, too, presses its claim to information, either through the agency of journalists, or as individuals. Since 1960, (d) the main meetings of local authorities have been public in the absence of a resolution to the contrary; and electors

(c) Local Government Act 1972 s.101 (8). The principal exceptions are education, social services and the police - s.101 (9)

(d) Public Bodies (Admission to Meetings) Act, 1960, and Local Government Act 1972 s.100

have the right to inspect various written records. (9) Recent planning legislation, too, has had the effect of increasing the requirement to publish information. (10) The effects of computerising the storage and flow of information within an authority adds yet another complication, one which by and large has not received much attention, at least so far as its non-technical implications are concerned.

2. Political tensions

The conflict between individuals' demands for privacy and the demands of the "public" (obviously comprising those same individuals) for openness in government, is by no means confined to local government, and has been analysed from various disciplinary standpoints. A Canadian lawyer, Professor Lawford, has expressed the view that access to government records is so essential to democracy that privacy rights must take second place. He regards computerisation as pernicious inasmuch that permanent records may not be created for the archives, and the circulation of information both within government and via the (sometimes unofficial) bridgeheads to the public can be more precisely controlled. (11) He favours a Freedom of Information Act, of the kind implemented in the U.S.A., concluding that: "No legislation should be enacted to protect privacy without such legislation to protect freedom of information". (12) The same general issue has been discussed by Friedrich, (13) McCombs, (14) and the Franks Committee. (15)

It is hard to imagine anything much more paradoxical than public control over what the public may not know. That scrutiny is desirable has been illustrated in the context of military security by the sociologist R.P. Lowry, who concluded: "I have theorised that security systems within that type of context ie., the Pentagon function both to undermine the purposes for which they were originally intended and, consequently, to take on additional functions which were unintended and undesired". (16) Similar temptations

could arise in local government. An obligation not to disclose for privacy reasons could be misused in order to conceal indications that administration had been below standard: being able both to conceal information and to cite a socially responsible reason for doing so could make deception doubly effective.

A cyberneticist, Stafford Beer, takes a different view of the same problem area. He sees the tension as lying not between governors and governed, but between the "esoteric boxes" of organisations. (17) Since the esoteric boxes seek their own stability and independence, they resist the development of any "meta-system" which would coordinate their activities - which would necessarily involve the divulging and sharing of information. Institutional possessiveness sets in. Jensen has described the phenomenon in more prosaic terms as "bureaucratic vanity": "an almost mercantilistic ambition towards becoming self-sufficient ... agencies are disinclined to ask other agencies for information, they obviously seem to consider it as a sign of weakness". (18) At first sight, the effect would seem to be to enhance privacy protection. However, Beer's thesis is that we urgently need to strengthen the meta-system: this being so, success would cause the privacy protection to disappear.

3. The role of the computer

Given the wide range of activities carried on by local authorities, the opportunities for what might be termed "ad hoc" computerisation are numerous. Every authority has its treasurer's department, dealing with inventories, billing, payment of wages, and other routine accounting operations which are essentially the same as in commerce. Other functions require the compilation of personal dossiers, which are more particularly a characteristic of public administration. Property information is needed in

systemised form, for rating and planning. Research departments may want to run computer simulations, or analysis of statistics.

At the hub of all these different demands lies the treasurer's department. It is here that the computer will have been established and reared on accounting functions. As the computer provides a service to a wider range of departments, the role of the treasurer/computer department has to change. Independent and conflicting demands come from all directions and deciding which of these are to be met calls for a technical-political process, trying to relate what is technically feasible to the organisational requirements.

In this kind of environment, it is difficult to see how privacy protection can be developed subject to an overall strategy. However, some confident predictions have been made that such "ad hoc" computerisation is not the way of the future, but that an authority should develop integrated database facilities, capable of meeting the needs of all the different departments, at the same time allowing rationalisation of data collection and storage.

Such ideas were far-fetched in the batch-oriented days of a decade ago. For example, a conference of local government computer users in 1960 (19) treated a number of computer applications as a quite separate basis, indicating that any sharing would be by the exchange of documents. (e)

(e) "Dr. Wrigley emphasized that the confidential nature of many medical records and said he would not be prepared to allow transit of these documents to other departments" (emphasis added) Ref (19) at p.32.

However, in America in the mid-60's, some ambitious projects for integrated information systems were launched. These included Santa Clara County's LOGIC system, (20) the "People Information System" in Alameda County, (21) and city-based systems in Detroit, (22) and New Haven. (23) In many cases the objectives and dealines proved unduly optimistic, leading a professor of Public Administration to comment, in 1968: "Theory, as represented in the literature of Urban information systems, is seriously at odds with what actually exists today". (24)

This general opinion was shared by Westin and his team, following their questionnaire and site surveys which included several local government installations. (25)

So far, the only system really to make headway towards integration has been that of the Municipality of Wichita Falls, Texas. (26) This has a relatively small population (100,000), the aid of substantial USAC (f) funding, and even so the system is far from complete.

Other projects have tended to concentrate on advancing data collection and filing techniques to the point where they can better support an integrated system. Most use property-based files. Thus Hogan (27) has reported on an IBM system to digitise and search property records for the City of Alexandria, Virginia. Projects to geo-code properties within urban local authority areas have also been inaugurated in England, including Coventry, (28) Bradford, (29) Newcastle-upon-Tyne, (30) and Leeds. (31)

(f) Urban Systems Inter-Agency Committee (9 federal agencies are represented).

Although a number of English authorities have computerised person-based files for their child health programmes, welfare services, or other activities where retrieval by name is needed, very little integration of such files has so far been attempted. Probably the nearest to this is the LOLA (g) project, in which compatibility between person-based files is being built in from the outset. (32)

4. Theoretical proposals

4.1. The underlying assumptions. A number of assumptions run through the literature outlining possible or predicted local government systems: (urban systems are the most frequently discussed).

Firstly, data for planning is assumed to be obtained as a by-product of routine administration. The reasoning is summarised by Cristiana et al: "The data used in planning and operation of urban government must be current and reliable, and there must be economical means for gathering such data. It has been concluded that gathering data during the operational course of government is the only possible way to meet these criteria". (33)

Secondly, data must be collected by different departments using definitions which are as compatible as possible. This may be justified in terms of "effective horizontal interactions between departments", (34) or simply because common definitions make it easier to prepare statistics. (35)

Lastly, there is often a basic assumption to the effect that the sheer quantity of demand for information is growing and will continue to grow. (36) The virtue of the computer in this respect is, therefore, its ability to

(g) London On-line Local Authorities (Hackney, Haringey, Hillingdon and Tower Hamlets)

retrieve required data items from very large files with speed and accuracy.

All three assumptions need to be questioned. Firstly, while it is undoubtedly wasteful to duplicate the collection of details of property or rate payments or other standard items, it is not necessarily the case that information required for administrative decision-making is identical with that from which plans are best formulated. For example, it may be pointless to site a new park in a position offering quickest access to the maximum number of probable users, if many members of the community have a prejudice against visiting that site. A quick survey of local attitudes may be more useful than a multi-factor computer analysis. (h) Also, the fact that the administrator has to deal with day-to-day events does not mean that all his records are kept up to date. If a newcomer joins the household in a council property, this may be unknown and of no consequence to the housing department until, say, an application is made for a transfer. Meanwhile, the out-of-date data on the inhabitants will remain on file. Only a limited number of functions (such as rent rebates, reviewed periodically) require regular status reports on or from individuals.

Secondly, although common data definitions may be agreed formally, it has to be noted that, particularly with personal information,

-
- (h) An instance of this kind is cited by Weiner, though without any precise reference. Recreational centres were located by an accessibility study, and several had later to be closed. "The interests, habits, preferences and group dynamics of the Negroes living in the neighbourhood affected were not taken into consideration". (37) The Birmingham Parks Department habitually consults with local social workers on decisions of this kind.

- (i) interpretation and idiom will vary from department to department
- (ii) context-data will also vary (eg., divulged or observed, given in confidence, vouched for by signature, etc.)
- (iii) information will be given for a particular purpose: its exact relevance to that purpose will determine how complete and free from distortion it is.

Thirdly, it is all too easy for the acquisition of data to become an end in itself. Since personal information frequently has to be sought from the individ, any element of collecting information merely to meet the appetite of the system for current data must be resisted. This conflict of interest is most apparent in suggestions for "omnibus forms" for local authorities, (38) which could well result in more people providing more information at more frequent intervals than hitherto. A limited amount of rationalisation might assist the individ, (1) but the systems advantages ought to be coincidental.

One final assumption perhaps needs to be brought into the open. This is that the computer, as a dispassionate and logical tool, necessarily introduces rationality into decision-making. (j) At best, the computer can help along decision-making which is already being approached rationally.

-
- (i) The DHSS hopes to coordinate some pilot projects for forms covering eg., rent/rate rebate and supplementary benefits, in 1974. Letter from DHSS, 3rd August 1973
 - (j) For example, Jakobsen (ref 35 (c) at p.20) describes computers as "a powerful weapon against irrational political or administrative decisions".

But since politics so often works through compromise, it cannot always be assumed that rationality is a crucial factor, except perhaps in the broadest sense. The immaturity of the systems approach to many real-life decision situations has been neatly analysed by Churchman. (39) Extending this view to privacy protection itself, it is possible that a system offering substantial practical benefits and having, by any rational standard, a comprehensive set of privacy safeguards, might nevertheless be rejected as too threatening by the population at large.

4.2. Proposals in the U.K. With these pitfalls of the information system approach in mind, it is proposed to examine briefly two major studies published recently in this country. These are the Department of the Environment's G.I.S.P. system, (40) and the LAMSAC "Phase I" study. (41)

Much of the LAMSAC report is taken up with appendices listing file contents for an imaginary authority of 0.5 million population. The preface candidly admits that since all the possible local government functions are included, no such authority could actually exist. (42) The result is, however, that the two-tier division of responsibilities seems to be regarded as a departure from the ideal. Conversely, if all the files are correlated to the degree outlined, the functioning of the two tiers is bound to merge. While this may make some sense in management terms, it destroys the separate political identity of the two types of authority. The intertwining of administrations could make it impossible for councils elected with different political commitments to show any real mutual independence, and electors might well feel disenchanted with voting for what were essentially the two pairs of legs of the same pantomime horse. These considerations tend to be overlooked in discussion of the advantages of cooperation. (43)

Even if the LAMSAC Scheme is accepted as being completely hypothetical, it is open to two serious objections.

Firstly, it posits almost every conceivable cross-linkage. Council house tenants records would be linked to social welfare records, the purpose of the latter having been defined as "... to provide data to case worker for case management". Medical history would also be linked in. (44) School records of pupils would be linked with their parents' social services records. (45) It is pointless to propose these linkages, if later one has to recognise that they cannot be exploited because to do so would create too powerful a surveillance system.

Secondly, little attention is given to the cases where data is contentious, such that later referral to it may require hard copy evidence, including perhaps a signature. On-line updating of the waiting list in the presence of the applicant (44) might be advantageous in some instances, for example, but in others a document might have to be retained on file, meaning that both machine-coded and hard-copy files would be created. Once the need for hard-copy has been established, the computer must offer more attractions in order to justify itself. It could be that computerising the waiting list (as opposed to the list of available properties) offered no net advantage.

In contrast to the LAMSAC study, the GISP report starts from the planning-data requirements of a local authority. Centralisation of information storage and a reduction in ad hoc information exchange between departments are seen as a collateral effect of adopting GISP. (47) The more detailed implications for the acquisition and processing of operational data are recommended as a subject for further study "in the context of the development of GISP". (48) An emphasis on compatibility and cross-linking of data is again evident, but it is assumed that areal aggregates will often suffice, and the report devotes a lot of attention to problems of

establishing workable common areal units. (49)

The two reports take different views of integration, with GISP linking data to its "Basic Spatial Units", and LAMSAC proposing both property-based and person-based linkage of records. Further consideration is evidently needed as to how much integration is actually wanted by the administrative user, how much by the planning or research user, and to what extent their requirements overlap. When this has been determined, it may still be desirable to cross-link by different means for the two kinds of user, since the confidentiality problem for each is quite different, and, as Mindlin has suggested, (50) such separation may save a lot of trouble in implementing confidentiality control.

5. Shared Use

The Maud Committee in 1967 declared itself in favour of the wider use of computers, and recommended that where one authority could not justify its own installation, "joint arrangements with other authorities should be established". (51)

Sharing can be of three kinds:

- (i) a service agreement. Authority A either has on-line access to the installation run by authority B, or submits jobs for batch processing. For example, Warrington has a terminal to the Lancashire County Council computer, and various districts and boroughs are on-line in Nottinghamshire and West Sussex. (52)
- (ii) a partnership agreement. Two or more authorities set up an installation as more or less equal partners. Examples are the Chilterns Joint Computer Committee and LOLA. (53)

(iii) a regional database. This is an extension of partnership to provide a repository of planning information covering quite a wide area, with routine dp operations still being carried out independently. This has been attempted in the East Midlands, (54) and is the kind of installation which one anticipates will be set up on a more formal basis by the new metropolitan county authorities.

Apart from sharing hardware, authorities using the same kind of machines may wish to collaborate in developing software, as happened in the case of Hampshire, Wiltshire, Hertfordshire and Southampton. (55)

Legal authority for sharing and selling computer services is provided by the Local Authorities (Goods and Services) Act 1970, s.1 and the Local Government Act 1972, s.101.

Sharing is likely to be most attractive where population is thinly distributed throughout a number of authorities. Hence quite extensive collaboration is envisaged amongst the Welsh authorities. (56) Regional computing centres for local authorities are also the norm in Denmark, which has few major population centres. (57) However, one local government officer has predicted a trend to regional centres in more general terms. (58)

So far as privacy protection is concerned, a lot will depend on the way in which the joint holder-users of a shared information system choose to assign the responsibility for the operation of the system. On the one hand, the computer centre could acquire too much autonomy, so that privacy controls would be left to the discretion of the director of the centre.

Alternatively, the participating authorities might all wish to reserve the right to assert controls, leading to conflicts in their requirements and probable deleterious effects on the efficiency of the system. In the case of a service agreement, more than one authority might participate as a "customer", and suitable controls must therefore be agreed as between customer and customer, as well as between customer and provider.

Because of these problems of jurisdiction, it is likely that shared use will give rise to numerous difficulties in exercising privacy controls in the context of local government computing.

PREFACE TO PART II

Part II comprises four studies of the way personal information is currently handled in departments of local authorities, with a particular emphasis on the position in Birmingham.

The studies cover:

- Chapter 6 Social Services
- Chapter 7 Housing
- Chapter 8 Education
- Chapter 9 Rating and Finance

The principal responsibilities omitted are Public Health (due to be radically reformed in 1974) and Public Works, where it was felt that isolating the personal-information flow would be beyond the means of one researcher. The role of personal information in planning remains an important issue nevertheless, and is discussed elsewhere in this thesis.

Few cases were found of computerised files being already in existence. Much of the time the investigation began with the questions: what personal information is being held now, and what are the prospects for computerising it?

A much more difficult question followed: what means are used to protect confidentiality now, and how would computerisation alter these protection requirements?

Each chapter presents first of all a summary of the law relating to record-keeping by the department, followed by a survey of working practice in handling personal information, based on interviews and, in some cases, direct observation.

The overall conclusions from the studies are presented in Chapter 10.

CHAPTER 6
SOCIAL SERVICES

1. Introduction

Social work is a difficult field to legislate for. No-one can anticipate the million and one different situations which may be brought to a social services department, nor would there necessarily be a very high rate of agreement over the best kind of response to be made. The powers and duties conferred on a local authority therefore tend to be defined in the most general of terms, with the result that a lot depends in practice on the policy of the authority and the initiatives of its paid officers.

For example, a local authority is duty bound to bring care proceedings in respect of a child where it appears that there are grounds for doing so, (a) such a duty is nebulous in the extreme, and it is difficult to envisage, for example, mandamus being issued except in the most flagrant cases. It is against this background of indistinct duties that one has to set requirements (as found in the same statute (b)) "to cause enquiries to be made", or otherwise acquire information.

The problems are not only those of definition, but of demarcation. In the past few years, there have been rapid moves towards the integration of social services. First the Seebohm Committee recommended the abolition of the distinction between services to children, the mentally ill, and "welfare" (mainly the elderly). The recommendations prompted the Local Authority Social Services Act, 1970, which did away with the statutory requirements to

(a) Children and Young Persons Act, 1969, s.2 (2)

(b) Ibid, s.2 (1)

maintain separate committees, and introduced a single requirement for a social services committee. (c) In parallel with this, attempts have been made to integrate the treatment of problem children, across a wider front; this was recommended by a White Paper in 1968, (1) and enacted in the Children and Young Persons Act, 1969. However, progress here has tended to be slower, given the greater autonomy of the agencies concerned, and the advent of a government less sympathetic to the philosophy of the original White Paper.

Integration ought to eliminate problems of demarcation, but in practice it often merely shifts them to a different organisational level. Thus a social worker, although no longer labelled "welfare" or "children", may still see a family as a housing problem or a child as a case best dealt with by the police. Whilst the various agencies may collaborate in order to avoid duplication of effort, in the last resort they all work with finite resources, and do not wish to shoulder responsibilities which appear to belong elsewhere.

2. Legal background

There are few legal requirements for a local authority to keep social work records. Case records must be kept on children boarded out, and these must be retained for three years after the child reaches 18, or dies. (d) Recent legislation has created the duty to collect information concerning the

(c) Local Authority Social Services Act, s.2 (1)

(d) Boarding-Out of Children Regulations, 1955, reg. 10(s), made under s.14 of the Children Act, 1948

chronically sick and disabled, with therefore an implied duty to store the information. (e)

In various situations concerning children, the authority may be under a duty to make enquiries, and again the natural outcome will be the creation of a file entry or reports on the child.

Investigations may be required to establish if care proceedings should be initiated, (f) or to assist the court in proceedings which are pending, (g) or in progress. (h) Once an authority has taken a child into care, or assumed parental rights, (i) it will inevitably build up its records on the child's progress.

An obligation to inform the local authority of a limited number of details about a child (principally name, date of birth, and address of parent or guardian) is laid on foster-parents; (j) there is also an obligation to notify in respect of protected children, placed pending adoption. (k)

-
- (e) Chronically Sick and Disabled Persons Act, 1970, s.1 (1), (in force, October 1971). For accounts of how information collection has been organised, see Local Government Chronicle 25th September 1971, p.1690 and 9th October 1971, p.1822. See also 1970 Act s.21 (5)
 - (f) Children and Young Persons Act, 1969 s.2 (1): also (where parents press for proceedings), C & YP Act, 1963 s.3 (2)
 - (g) C & YP Act, 1969, s.9 (1)
 - (h) Ibid, s.9 (2)
 - (i) Children Act, 1948, s.2 (1): C & YP Act, 1963, s.48
 - (j) Children Act, 1958, s.3, modified by C & YP Act, 1969, s.53
 - (k) Adoption Act, 1958, s.40

The authority must establish the religious persuasion of parents in assuming parental rights itself, (m) taking into care, (n) allowing relatives to take over the care of the child, (o) or in fostering the child. (p)

In adoption proceedings, a director of social services may be appointed as guardian ad litem for the child, with the responsibility of preparing a full report on the home background. The report is submitted to the court confidentially: (q) this requirement can act contrary to natural justice, and several appeal cases have resulted. "Confidential" in this context has been held to mean "at least that the parties are not automatically as of right entitled to see the report or be informed of its contents". (r) The rule has been justified on the "candour" principle, (s) (discussed earlier, 3.6.4.) but the right of the judge to disclose all or part of a report to a party to the action has been repeatedly upheld. (t)

Should information from local authority records be required in adoption proceedings, a 1968 Practice Direction allows the court to treat the

-
- (m) Children Act, 1948, s.3 (7)
 - (n) C & YP Act, 1969, s.24 (3)
 - (o) Children Act, 1948, s.1 (3)
 - (p) Boarding-Out Regulations ((d), supra) reg. 19
 - (q) Under Adoption Rules for: County Court, r.9 (2), Juvenile Court, r.9 (2), High Court, r.15 (2)
 - (r) Pearson L.J. in In re G (an infant) [1963] 2 Q.B. 73 at 99
 - (s) Sachs L.J. in Re M [1972] 3 All E.R. 321 at 329
 - (t) Including Re M ante. See also Donovan L.J. in In re G ((r) above) at 97; Lord Denning M.R. in Re P.A. (an infant) [1971] 3 All E.R. 522 (both county court hearings): Roxburgh J. in Re J.S. (an infant) [1959] 3 All E.R. 856, (from juvenile court)

information as confidential. (u) In Re D (1970), (v) a mother sought the return of her two children, who were wards of court and fostered with a county council: counsel for the mother successfully sought the production of a child care officer's notes on the children. The Court of Appeal ruled that this was undesirable, with Lord Denning stressing the need for child care officers to be "completely free and frank", (w) and suggesting that since the records in question were to be kept for inspection by persons "authorised ... by the Secretary of State" (x) they were in effect privileged. It is submitted that this latter argument could be capable of undesirable extension.

The social services department may be called upon to provide a welfare report in juvenile court proceedings against a child, and such reports are deemed confidential, though material parts should be read or summarised for the child or the parents. (y) In the view of some practitioners, as much information as possible should be communicated in this way. (2)

3. Shared use of records

Records in a social services department range from lists of clients' addresses to highly subjective comments kept in the social worker's desk drawer. Nevertheless, a good deal of personal information has to be put on formal records, if only so that cases can be handled by colleagues when a worker takes time off or moves to another job. There is therefore always the possibility that the information will find its way into someone else's report to another agency or in connection with legal proceedings.

(u) Practice Direction [1968] 1 All E.R. 762

(v) [1970] 1 All E.R. 1088

(w) Ibid at p.1089

(x) Ibid at p.1089

(y) Under the Magistrates' Court (C & YP) Rules, 1970, regs. 10 and 12.

The BASW view is that information obtained for one purpose should never be used for any other without the consent of the client. "If agencies, for administrative convenience, and also thinking they know "what is good for the client", act without reference to him, they will destroy the confidential basis of casework ..."(3) A conflict can therefore develop between what the social worker sees as a breach of trust, and the administrator sees as a process of rationalising wasteful duplication of data collection and recording. The issue was apparently one of the foremost to be discussed at a social services conference in 1970. (4)

Conversely, it has been suggested that social services departments should draw on the records of other departments. The Seeborn Committee felt that the records of general practitioners and the DHSS could help in identifying elderly people in need, although it qualified its recommendation by saying that the permission of the individual should be sought. (5) The release of details of handicapped people from Department of Employment registers has been urged, (z) and denial of such information from government records has been described as "paying too high a price for our passion for privacy". (a)

4. Research and Planning

A research and intelligence unit serving all local public services was recommended by the Seeborn Committee, (6) who also recommended particularly close planning links between social services and housing. (7) Clearly such collaboration would involve the pooling of information, though much of it

(z) by the Chief Welfare Officer, Croydon L.B.C. Local Government Chronicle, 20th March 1971, p.475

(a) by the Clerk to Cheshire County Council, Local Government Chronicle, 24th November 1972, p.2037

might be statistical only.

Social service records may also be of interest to sociologists and medical researchers. An example of how data ought not to be acquired was provided by an American study, where the records of a defunct psychiatric clinic were found to be taking up space needed for other purposes in a hospital; the records were handed over in toto to a medical school, where researchers proceeded to follow up children who had shown signs of maladjustment, to see if their adult life reflected this. Although the purpose of enquiries was concealed, their detective methods showed zeal of an extreme kind; thus when a relative protested; "He has enough trouble raising his kids and dogs without being bothered by you", the ex-patient was promptly tracked down via the local Kennel Club. (8)

A more responsible technique has been devised for a study carried out jointly by the M.R.C. Social Medicine Unit and Tower Hamlets L.B.C. over the past few years. The study's aim is to correlate the factors which contribute to juvenile delinquency, (9) and so it is essential to be able to cross-link the records from Tower Hamlets' courts section with others from the schools, courts and probation service. However, all the linkages are made by an independent third party, who maintains a list of names and code numbers. Records reach the M.R.C. with only the code numbers. (10)

5. Empirical studies

It was felt desirable to obtain some first hand appreciation of the handling of personal information in social services departments. Accordingly, visits were made to the records sections of the social services departments of Birmingham C.B.C. and Tower Hamlets L.B.C. A more detailed study was made in a local office of the Birmingham department.

5.1. Central records. Central record-keeping tends to be complicated by the legacy of indexes from the different constituent groups in a S.S.D., each of which may have used a different system. Also, records relating to young offenders require separate handling, since the fairly detailed information has to be compiled in collaboration with other agencies. Whereas a simple card index will suffice for an old people's register, the courts section must resort to a good deal of form filling and duplication. It may have to create the necessary documentation to pass on to someone carrying out supervision, or to keep for reference in the event of an appeal. Furthermore, a child may live in the area of the S.S.D. but commit an offence within the jurisdiction of a court elsewhere.

As well as hard data, agencies will quite often exchange warnings or hunches, in conversation or by telephone. Much of this never goes onto the files, but may induce someone to specially retrieve or re-scrutinise a record. In the case of suspected "battered babies" in the Birmingham area, doctors are invited to send the S.S.D. a special card giving the parents' name. They will then be told if any other notifications have been received. Anyone featuring several times on this file will obviously be treated with suspicion, but the file itself does not state or prove anything.

5.2. The Area 9 Study.

5.2.1. Background. Birmingham has devolved its social services provision to twelve area teams, each of which therefore corresponds in scale with the expectations of the Seebohm Committee. (11) Area 9 is based in the South-east of the city, at Acocks Green, and covers the declining inner ring areas of Small Heath and Sparkbrook, as well as the more prosperous immediate neighbourhood of Acocks Green itself: (see Appendix II for map). At the

time of the study, 37 caseworkers were based at this office, with a small proportion of these working part-time, or dividing their work between Area 9 and another agency. An administrative team of six dealt with enquiries, filing and accounting. Five secretaries were responsible for the typing of forms and of outgoing mail. Responsibility for the day-to-day running of the Area lay with the Area Officer and his assistant officer, who would be drawn into individual cases only where they presented particular difficulties.

Cases might be referred to the office by the client in person, by a councillor, doctor or by official or voluntary bodies. Initially the case would be handled by the Intake group, being passed on to Long-term if extended casework was felt to be necessary. Decisions for allocating these cases, and for dealing with special responsibilities such as fostering or adoption, rested with five senior social workers.

The office held case files on about 1500 current cases. A card index of current cases, showing the date of referral and one or two basic details of each case, was kept near the telephone switchboard for quick reference.

5.2.2. The Communications Study. A study of the communications to and from the area office was carried out over a period of six weeks.

The aims of this study were:-

- (i) to gain an appreciation of the information requirements of social workers, and of the reasons for which they might wish that this information be treated as confidential

- (ii) to assess the approximate amount of information about individuals exchanged between area 9 and other agencies on a regular basis.
- (iii) to identify particularly the information flow within the local authority.

From these assessments, it was hoped that a realistic impression could be formed of the prospects for introducing computerisation in such an office, and also to assess the restraints on access which would be consistent with current practice.

Method. The staff were naturally concerned that the study should not itself infringe the privacy of clients. Accordingly, the following approach was devised to meet this concern. Before the survey was begun, the method proposed was discussed personally with every member of the staff to be affected.

Telephone communications. All incoming calls were routed through a single switchboard. The calls received by each social worker were logged over a half-day period. Details of the calls were sought from the workers in the following half day. Problems of recollection were few, arising mainly where the person concerned had been out visiting clients and so could not be interviewed until a day or two later. By this method, each person could indicate as much or as little as he or she wanted to, about the content of the call.

The key question was always: did the call concern one particular client? If so, it could be assumed that personal information about that client was being exchanged. In many cases, this was not the kind of

information which would be entered on file. Also, a call might develop into a lengthy consultation or negotiation. However, the study proceeded on the assumption that where exchanges occurred frequently between Area 9 and another agency, there would tend to be a mutual interest in the information held on files, such that shared retrieval facilities might eventually be an attractive proposition.

After the second week, the staff expressed willingness to allow direct observation of their outgoing calls, with the observer sitting at one of the desks and logging each call. In due course many of the staff helped in a positive way, for example by calling across that the call was to X and concerned a client.

Certain kinds of call caused difficulty. Where an outsider rang in and simply asked to be 'phoned back, the resulting outgoing call was treated as the only event. Similarly, if several attempts were made to call someone who was not available, these unsuccessful calls were not recorded even though the agency may have given some kind of answer. Where calls were made with a client in mind, but with no actual mention of him by name (for example, in seeking a vacancy in a children's home) this was counted as not involving personal information.

Letters. The secretarial staff agreed to record the destination of letters, and whether they related to particular clients. They also indicated if the letter was by way of an inquiry or a reply.

Handwritten letters, usually sent by caseworkers to clients to advise of an impending visit, were not included. Nor could any method be found of monitoring incoming mail, without causing either undue inconvenience or infringement of confidentiality.

Limitations of the method. Most of the observations were for February, which experienced workers regarded as a time of average workload. However, the nature of casework does vary through the year: old people, for example, tend to need more attention in the winter months.

A study of just over one man-month cannot anyway claim great precision. However, the precision was regarded as adequate for the kind of broad assessments being made.

Results. The results of the telephone and letter surveys are summarised in Table 1. The relative frequency of contact between Area 9 and other agencies is shown in Table 2, and Figure 3. All the figures relate to communications about individual clients, which were found to comprise 86% of the letters and 90% of the telephone calls.

Two general conclusions are:

(i) Quite a lot of communication is concerned with locating where responsibility has been assumed for people in difficulties, or where information is being held on them. This is suggested partly by the 7% of incoming telephone calls which had to be re-directed to other agencies (usually a neighbouring area), and the further 7% which were dealt with by reference to the card index by the switchboard. Also, quite a number of telephone calls made by social workers were of the form "are you dealing with Mr. X?", or other enquiries designed to ensure that responsibilities were not overlapping. Central computer records therefore, might aid the coordination of services, by indicating which agencies were dealing with which clients, without necessarily holding more than identifying information about each client. This becomes a particularly attractive prospect when the different agencies all use widely differing areas as units of administration (see Appendix II).

(ii) By far the largest outside group communicated with was found to be the medical profession. NHS doctors and medical social workers accounted for 22% of incoming calls, 14% of outgoing calls and 16% of outgoing letters. The absorption of some Public Health services into the NHS in 1974 will no doubt increase this proportion.

Conclusions. There would seem to be little incentive to computerise the case records held by an area office. However, Figure 3 suggests that area offices could derive benefit from on-line access to computer files which might be set up in centralised offices, such as Housing and the central Social Services Office. Dial-up links to hospital files might also have attractions, but the technical and inter-professional difficulties are greater.

The figures make certain negative points. There is relatively little contact with the D.H.S.S., for example, and virtually none with other government departments. The overall level of communication activity is not all that high, leaving one with an impression of regular but low-powered contact between Area 9 and eleven other agencies.

Table 1 Telephone calls and letters. Area 9 Office

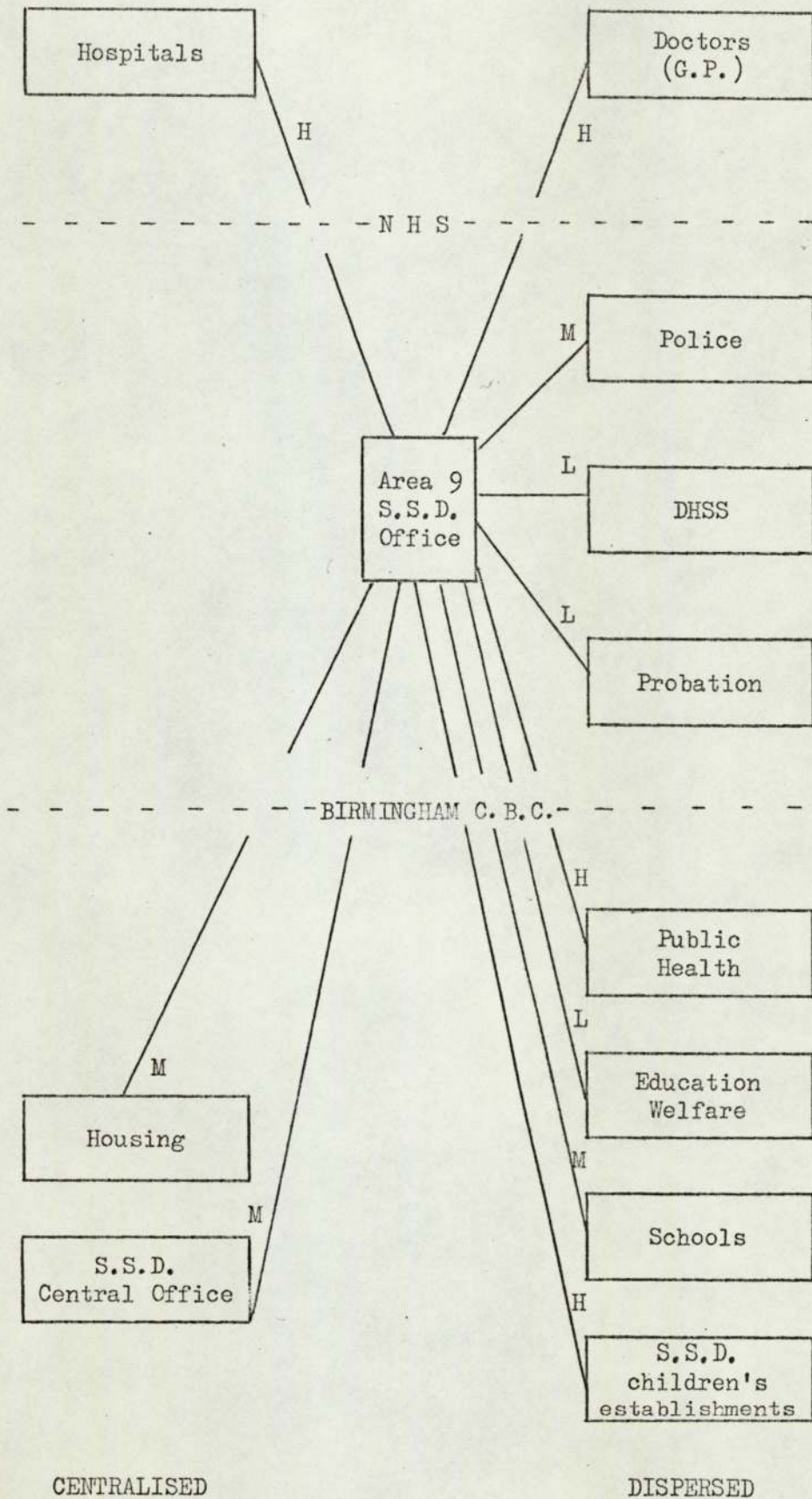
To or From	Outgoing tel. calls, 4 days, <u>not</u> senior staff	Incoming tel. calls, 4 days		Letters, 10 days All staff		
		All staff	Not seniors	Inquiry	Reply	Total
1. <u>Clients</u>	41	67	62	31	21	52
2. <u>Birmingham C.B.C.</u>						
S.S.D. children's establishments	24	13	12	-	-	-
Public Health S.S.D. central office	19	11	8	1	-	1
	19	14	5	2	3	5
Housing	15	4	4	8	5	13
Schools	9	10	8	1	2	3
Other S.S.D. areas	5	6	6	2	2	4
Education Welfare	3	6	5	-	-	-
All Others	19	4	3	-	-	-
TOTAL	113	68	51	14	12	26
3. <u>Other agencies</u>						
Hospitals	18	16	14	2	2	4
Doctors (G.P.)	11	14	12	13	2	15
Police	15	11	11	-	-	-
Other S.S.D's	5	9	6	4	6	10
DHSS	7	6	6	5	1	6
Probation	5	2	2	-	-	-
All others	27	11	10	5	4	9
TOTAL	88	69	61	29	15	44
Calls re-directed		17				
Calls dealt with at the switchboard		18				
GRAND TOTALS	242	239	174	74	48	122

Table 2. Area 9 Office: Relative frequency of contact with other agencies

<u>Agency</u>	<u>Telephone calls</u> (in and out, not senior, <u>4 days</u>)		<u>Letters</u> (outgoing, all staff, <u>4 days</u>)
S.S.D. children's establishments	36		1
Hospitals	32	(High)	2
Doctors (G.P.)	23		6
Public Health	27		0
<hr/>			
Police	26		0
S.S.D. Central Office	24	(Moderate)	2
Housing	19		5
Schools	17		0
<hr/>			
Other S.S.D.'s	11		4
DHSS offices	13	(Low)	2
Other S.S.D. areas	11		2
Education Welfare	8		0
Probation	7		0

Figure 3 Rate of contact between Area 9 and other agencies

(H = high, M = moderate, L = low, as per Table 2)



5.2.3. The Questionnaire. The observations in the Area 9 office created a number of impressions about the attitudes of social workers to privacy. In one way or another, they identified themselves strongly with the interests of their clients, which, while it might result in "possessiveness" with regard to private information on the case, could also mean that privacy restrictions imposed by other agencies were seen as restrictive, even signalling non-cooperation.

Discussion of cases within the office tended to be fairly open. Clearly some cases were so exasperating that discussion of them was a form of release. However, this relaxed and forthcoming approach only tended to be extended on the 'phone to other people working in a very similar role, such as the staff of a children's home, or health visitors.

In order to formalise some of these impressions, a questionnaire was circulated to all the social work staff of Area 9. A further sample was later obtained from the Area 12 office. Altogether 75 questionnaires were circulated, of which 34 were returned. Respondents were asked to complete and return the form in a pre-paid envelope, without discussing the questions with any colleagues.

It is probable that those who responded had a higher than average degree of concern about confidentiality. Also, a sample of this size can only represent opinion in the Birmingham environment. As with the previous study, the statistics are presented as being adequate for this thesis, but by no means as representing a general situation or offering fine discrimination in measurement.

Those who responded comprised: 9 senior staff, 14 social workers, 8 welfare assistants/trainees, and 3 no indication.

The questions and replies

Q.1. The N agency are suspicious about the income declaration made by one of your clients in an application to them. They suspect that the applicant's wife is working. You know this to be the case. Would you give information to the agency?

<u>Agency - in order of willingness that information be given</u>	<u>No</u>	<u>Would confirm that wife working</u>	<u>Would give details of wife's job & employer</u>	<u>Don't Know</u>
Housing Dept. (rent rebate)*	21	12	-	1
DHSS (supplementary benefit)*	21	12	-	1
Rates (rate rebate)	24	9	-	1
Inland Revenue (tax deduction)	25	7	1	1

Q.2. Mr. and Mrs. X are joint tenants of a council house. They have four children. You know that Mr. X had a violent row with his wife two months ago: he left home and is now living with another woman.

Indicate if you would give information to:

<u>Agency - in order of willingness that information be given</u>	<u>Would indicate X no longer living with his family</u>	<u>Would give Mr. X's new address</u>
Health visitor/clinic	29	6
Housing Dept.	27	5
Family G.P.	25	5
Education Welfare Officer	23	4
DHSS	25	2
Rates Dept. *	15	-
Police *	13	1
Debt Collecting Agency	7	1
Husband's mother	4	2
Wife's mother	5	1
Husband's employer	1	1
Husband's bank manager	1	1

11 respondents qualified their answers to this question. 5 said they would release the information only with the client's consent, 4 said that a lot would depend on the circumstances, and 2 said they would prefer to advise Mr. X to get in touch with the agency.

Comment on questions 1 and 2.

The replies illustrate how disagreements on the nature of the claim to privacy centre on situations where there is a case for over-riding privacy. The lack of unanimity in some of the responses is marked: for example, in the cases marked with an asterisk, there is not even a two-thirds majority for disclosure or non-disclosure.

Implicit in the comments volunteered in question 2 was the suggestion that the question was impossible to answer. Yet this is just the kind of question that has to be asked by anyone considering privacy controls on the basis of "authorised" access to "non-sensitive" data. Whether the lack of unanimity reflects differences of opinion, or differing interpretation of the question, the implications for trying to set up a systematic privacy control are much the same. Lest the example be regarded as too hypothetical in terms of computerisation, it should be noted that the data in both cases is simple and basic, and therefore of a kind that could well be recorded in, say, a centralised Social Services file.

Q.3. Do you feel that other agencies impose unnecessary restrictions on the information relating to your clients which they will give to you?

<u>Agency</u>	<u>Imposed never or very rarely</u>	<u>Imposed sometimes</u>	<u>Imposed frequently</u>	<u>Don't Know</u>
General Practitioners	11	18	3	2
Hospitals	9	18	3	4
Public Health workers	22	7	1	4
Probation Officers	22	6	-	6
Police	17	10	3	4

Comment on question 3.

The figures reflect a feeling expressed several times in conversation, that the medical profession tends to be over-secretive. The local authority employees in the Public Health field are, however, regarded as more cooperative.

This adds a further dimension to the policy issues raised by the previous question, since "playing it on the safe side" by putting tight restrictions on information may be resented by others who see access to the information as necessary for their work.

Q.5. Indicate the statement(s) which best indicates your reasons for protecting confidential information about clients, and indicate the one you regard as being of primary importance.

	<u>Chosen (but not primary choice)</u>	<u>Primary Choice</u>
"personal obligation to the client"	14	16
"need to create climate of trust in social work"	17	3
"sense of belonging to social work profession"	10	1
"desire to work within the Law"	3	-
"sense of duty as a public servant"	1	-

Comment on question 5.

The reasons chosen tend to be practical and personal, rather than based on more abstract concepts of law and duty. The emphasis on personal obligation to the client is particularly strong, suggesting that the social worker (as data collector) will identify strongly with the indid, and seek to impose restraints on behalf of the indid, rather than in furtherance of a broader policy.

Q.4. and Q.6.

Asked how often occasions arose when they felt that normal rules of confidentiality should be set aside for the benefit of the client, respondents divided evenly between "rarely" and "quite often". Justification for setting aside confidentiality in "the public interest" was generally felt to occur "rarely".

Asked to assess the probable impact of computerisation on social work, the majority response was anti-computer, with 19 replies agreeing that computerisation would make social work less personal, and the same number indicating that they thought computerisation would make the protection of confidentiality more difficult. Very few evidently thought the computer would bring improvements in either respect.

Conclusions

Three conclusions are suggested by the Communications Study and Questionnaire.

- (i) Social workers have a very lively sense of the personal ethics of disclosing information about their clients. They see the ethical decisions in terms of situations and individuals, and do not operate by rules of thumb. It cannot be assumed that any restrictions on data flow based on cataloguing or grading data will be appropriate for data originating in the social work environment.
- (ii) There is little correlation between frequency of contact and willingness to pass over information. It cannot be assumed that because two agencies have regular dealings with one another, they operate relaxed confidentiality policies with regard to information exchange.

- (iii) One way in which centralised computing might help social workers and others is in maintaining current lists of agencies' clients. However, access to even these lists could raise ethical problems in particular circumstances, and in more pragmatic terms, such a scheme would comprise a surveillance system, capable of cross-linkage with other local authority files and functions.

CHAPTER 7HOUSING1. Introduction

In the allocation and management of council housing, a local authority holds a strong influence over a large section of its electorate. Most housing policy rests on political decisions of the council, as translated into standard procedures and administered by the paid officers. Usually these officers will take a pride in making decisions on an impartial basis, but the tenant or applicant has few legal rights whereby he can insist on such fair treatment. Although an obligation rests on councils to house the homeless, (a) this tends to work only for extreme cases. Once a person is given a council tenancy, there is no security of tenure, and there is no obligation to continue a tenancy for spouses or children surviving the death of the tenant. (1)

Since housing administration involves decision-making which is largely discretionary, and which calls for assessments of the character and "suitability" of applicants, it provides an interesting case study of the way personal information is stored and used. Having somewhere to live is a matter of major importance to everyone, and so one would expect the pragmatic considerations to be uppermost. In this chapter, the preoccupation is with the balance between privacy claims and the need of the administrator to have fairly wide background information on his client. Clearly he ought not to have or use irrelevant information, such as the applicant's brother's criminal record, or the child guidance reports on the applicant's children.

(a) National Assistance Act, 1948, s.21 (1). London Borough of Southwark v Williams [1971] 2 W.L.R. 467

But there are grey areas of information which may be relevant and yet may be regarded as privacy-invading. If an applicant is turned down after consideration of such information, he is more likely to object because he thinks the result unfairly arrived at, than because he feels that his dignity or feelings have been affronted by the acquisition of the information.

2. Legal background

There is extensive legislation on the financing, compulsory purchase, and management of housing. Only three points will be mentioned here.

Firstly, authorities can use housing which is due for demolition, and therefore likely to be of poor quality, to provide council accommodation. This power was conferred by the 1954 Housing Repairs and Rents Act, s.2, (b) and results in a class of "1954 Act" tenants, who are often offered this kind of accommodation because their housekeeping standards are poor.

Secondly, the Housing Finance Act, 1972 creates a duty to give rent rebates to council tenants, and rent allowances to private tenants. (c) The rebate must take account of the needs of the tenant, and the authority may insist that "such information and such evidence as they may reasonably require" should be provided to support an application. (d) If an applicant

-
- (b) Since consolidated in part 3 of the Housing Act, 1957
 - (c) Under s.19. Allowances were extended to furnished tenancies in the private sector by the Furnished Lettings (Rent Allowances) Act, 1973
 - (d) Housing Finance Act Schedule 3, para 2 (1). For author's criticism of this requirement while the legislation was pending see Local Government Chronicle 14th July 1973, p.1192

disagrees with the finding, he can insist on a review and a statement of reasons. (e) A tenant is under a duty to inform the council of any change in his circumstances. (f) However, the effect of such requirements may be modified by directions issued by the Minister, for example that councils should not investigate too closely where an application is supported as a hardship case by a social worker: "No one should be dissuaded from pursuing an application by their fear of having to disclose personal details, in addition to financial details, to the officers of the housing authority." (g)

Finally, it must be noted that the housing responsibility rests, and will continue to rest, with the lower tier of authorities. Thus only in the metropolitan districts, toward which this study is oriented, will it be dealt with by the authority also handling education and social services.

3. Awkward tenants

Housing management necessitates a continual confrontation with a small proportion of tenants. They may fail to keep up with their rent payments, or overcrowd or damage their accommodation. The difficulties of dealing with such tenants were the subject of one of the Central Housing Advisory Committee's earlier reports. (h) The Committee urged collaboration between

(e) Housing Finance Act Schedule 4, para 15 (2)

(f) Ibid Schedule 4, para 3 (5)

(g) Department of Environment Circular 48/73, which introduces new areas of discretion with regard to private furnished tenants, in over-riding minimum residence period requirements. See paras 13, 19.

(h) CHAC, Housing Management Sub-Committee, 6th Report. "Unsatisfactory Tenants", HMSO 1955

departments (i) a call echoed by the Cullingworth report more recently. (j) But collaboration only adds to the complications of exchanging information. At what point, for example, should the Housing Department notify Social Services of a case of serious rent arrears? How much does the Department need to know about a tenant's illness which is allegedly causing disability?

The treatment of people in arrears has some parallels with the "social control" exercised by the National Insurance Section of the DHSS in collecting insurance contributions, as studied by Rule. (2) The final legal move, since the repeal of the 1938 Small Tenements Recovery Act, is an application to the County Court for payment or possession.

4. Dispersal

As well as meeting the needs of individuals, a housing department will aim to produce balanced communities, which have no preponderance of particular age groups, or awkward tenants, or immigrants. This means that an individual's entitlement will sometimes have to take second place to broader policy decisions, and that allocation will have to be based on knowledge of personal details such as age, rent payment record and race. The last factor is probably the most controversial. On the one hand a council may favour a "voluntary" approach (also advocated by a recent Select Committee report)(k) but any means used to prevent the concentration of immigrant groups constitutes in effect a positive dispersal policy. Such

(i) Ibid at para 39

(j) CHAC Housing Management Sub-Committee, 9th Report, HMSO 1969 para 106

(k) Select Committee on Race Relations and Immigration, "Housing", HMSO 508-1, 1971, para 115

policies have to be based on awareness of the race of tenants, which may therefore become a key characteristic on their files.

5. Empirical studies

Housing is regarded as a promising area for computerisation, and the computer applications developed by four local authorities are described in a LAMSAC report. (3) Some councils operate semi-automated systems, such as Camden L.B.C. where rent payments are recorded on paper tape and updated weekly by a computer bureau onto microfilm. (m)

In Birmingham, no housing files have yet been computerised. However, computerisation is being actively considered, and the more formalised and centralised administration of the department suggested that it would provide a case study with interesting contrasts with the Social Services Department.

The observations which follow relate to nine sections of Bush House, one of two major Housing Department offices in Birmingham. Bush House manages about 90,000 of the city's 140,000 council properties, and acts as the overall administrative centre for all housing responsibilities. These include the maintenance, building and demolition of housing stock, but this study centres on the allocating and letting of houses to tenants.

5.1. The Bush House study. It is necessary first to outline the functions of the different sections of the organisation which were studied. The accounts are based on 12 days of interviews at Bush House. The reader may find it helpful to consult figures 1 - 5 in conjunction with the text. The

(m) Visit of 13th July 1973. Copies of the microfilm are distributed to 8 collection points, leading to some problems of the disposal of obsolete films securely.

first four sections to be described are those which allocate housing to new or existing tenants; the Letting Section then actually create the new tenancy; the Arrears and Rebates sections handle accounting aspects of rent payments; and finally the Visiting and Tenancy Queries sections specialise in obtaining information for the other sections.

There are two files which are accessible to all the sections. These are the central registry, in which a case file containing all the documentation created in dealings with the Department is kept on every tenant; and the Central property register. This register can be interrogated via an intercom/TV screen system from most of the offices. Central case files are usually retrieved by a junior clerk, who will be despatched with a batch of standard slips of paper listing the names of the tenants.

Several of the offices divide their work into five sub-areas. These areas are standard throughout Bush House.

1. Applications Section

This section acts as the first point of contact for many members of the public. Quite a large proportion of them will simply be advised that their requests are unreasonable or that they are ineligible for Corporation property. The remainder will go onto the Bush House files for the first time.

Applicants are divided into categories based on their housing need. Special sub-sections deal with the immediate needs of homeless families, and with those who may be helped by housing associations. The main stream of applications are assigned to one of the "bedroom queues", and so join a priority list for properties having one, two, or three or more bedrooms.

Each queue is administered by a small sub-section, which maintains a card file, showing the priority of applicants in terms of housing "points".

The other files maintained for the whole section, are:-

- (i) a card file, arranged alphabetically by street and within streets by street number. This gives the name of the applicant living at that address, together with his registration number. Special cards are used to indicate change of address, and applicants dealt with by reference to housing associations. Free form comments may sometimes be entered on the card.
- (ii) Several shelves of case files, kept in orange folders, and arranged alphabetically by name. These total about 14,000.
- (iii) a card file, arranged by name, of those who have made enquiries but who will not fulfil the residence qualifications for a while. This is the Register of Enquiries, or R/E file, total, about 11,600.
- (iv) box files are used for two categories of awkward cases: these are
 - (a) applications where there is doubt about eligibility so that further enquiries must be made, and
 - (b) applications where nothing has been heard from the tenant for some time, (usually 2 or 3 years)
- (v) the section has three TV consoles linked to the central register of Corporation properties.

- (vi) an applicant who appears to meet the eligibility requirement will usually be visited by a Housing Visitor, who will assess the nature and living standards of the applicants' current accommodation. The Visitor's report is filed by applicant's name, in a Kardex tray system.

By far the widest range of information is kept in the case files. When applicants become tenants, these files are transferred to the central registry where they may later accumulate numerous documents from transfers, rebate applications, and so on.

The least information is kept in the street-indexed card-file. For much of the time, this is used to expedite access to the case files. By checking against the address, the clerk can see how the name is spelt, what the initials are, and indeed whether an entry exists for the address at all. Although every applicant is given a registration number, and this is entered on the address file, the use of the number as an identifying parameter has long since been abandoned. It was found that people rarely remembered it, nor would they find it when required, and for a section dealing with telephone enquiries much of the time, address has proved best identifier. A further benefit is that the registration of two people from the same address immediately suggests that the earlier registrant should be re-contacted if possible.

Confidentiality of information arises mainly with regard to:-

- (a) the visitors' reports. These give an assessment of the applicant's suitability for modern or older housing stock. The visitor gives various ratings of cleanliness, upkeep of garden and other aspects of the applicant's way of life. Free-form comments on the back of the form may be included.

- (b) the case files. Even at an early stage in processing an application, it may be necessary to seek certification of a marriage separation or other documents relating to a person's circumstances. The sensitivity of such documents (or the photostats of them) may lie in their ability to confirm and add detail to what another agency may only suspect.
- (c) telephone enquiries. With a high rate of telephone enquiries, from a wide range of callers, it is not always easy to test the validity or authenticity of requests for information. On some occasions, those dealing with an enquiry seemed afterwards to be a little uncertain of the status of the enquirer.

2. Overspill Section (Figure 1)

Both private and municipal tenants may apply for housing outside Birmingham area, either in the new towns of Telford and Redditch, or eleven "expanding towns" which cooperate with the city.

As with applicants for Birmingham property, a visitor's report is required. This may be of particular importance to the applicant, since most of the properties available are new, and a favourable assessment of living standards is needed.

Coordination with the Department of Employment over finding jobs in the new area is called for, but this does not appear to involve any direct exchange of personal information between Bush House and the Department.

House purchases are dealt with by the same section. Following a council decision to stop further sales, the only responsibility outstanding is that of keeping track of payments, and possible re-sales, for houses

already sold. A certain number of houses built specifically for selling at Chelmsley Wood, come on to the market from time to time. Anyone purchasing a home agrees to have his income checked with his employer, and municipal tenants can expect their case files to be checked for any history of rent arrears.

The main file used by the section comprises the cards filled in by applicants, arranged in name order, with edge markings to indicate the preferred Overspill Area.

3. Re-housing Section (Figure 2)

When housing stock is to be demolished in redevelopment areas, the Corporation accepts an obligation to re-house the private and municipal tenants affected. The negotiating position of such tenants is rather stronger than for other applicants for municipal properties: this can be a particular problem if the tenant is in arrears of rent in a council house, or has very specific ideas on the kind of house he or she wishes to move to.

The section collaborates closely with the Public Works Department, who produce Unit Plans showing the property to be cleared in a particular year. There may also be extensive cooperation with Public Health or Social Services workers over particular cases.

The files used by the section are:

- (i) the Unit Plans. Each of these has a number, which appears in all the Section's files.
- (ii) Kardex trays. The section divides its work by the five sub-areas

of the city covered by Bush House. Each area has its own Kardex tray, comprising visitors' reports and other information regarding offers of accommodation made to the tenant.

- (iii) case files. The section, alone among those studied, retains the case files of municipal tenants throughout the processing of their re-accommodation.

Reference sheets are also compiled for each Unit Plan, showing the address and resident of each property, together with an indication of the kind of accommodation for which he has been assessed as being suitable. Copies of these sheets go to four other sections, including Visiting.

The actual process of slum clearance is handled by a separate section, which collaborates close with the Public Health Department, and is the only section, apart from Rebates, to be able to require the production of information by law. This relates to people having an interest in property, under s.170 of the Housing Act, 1957.

4. Transfers Section (Figure 3)

The section again works with five teams, each covering one of the Bush House sub-areas. Each team maintains two card files:

- (i) an index by street/street number. This shows the applicant's name, bed queue, priority, and date of registration
- (ii) an index comprising the application forms, and arranged by bed queue and priority. The priority system is quite different from the points system used in Applications Section, and is based on a standard table. Applicants are rated according to the one factor which places them highest in the table.

The initiative for a transfer may be made by way of a telephone call, letter or personal visit. In all cases, the tenant fills in the standard application form, which is then processed as indicated in figure 3.

The section also handles exchanges of tenancy, which may become quite complicated if the opportunity is taken to free a house which is really larger than either of the tenants needs, or if lodgers are involved.

5. Lettings Section (Figure 4)

The section handles all the stages of allocating houses to new tenants, and completes the procedure when an offer made by Re-housing or Transfers has been accepted. It keeps track of the municipal properties which are available for letting, and spends much of its time preparing lists of these properties for circulation to other departments.

The only files kept by the Section are the registers of new, "1954 Act", and other municipal properties, and the case files used by the Tenancy Queries sub-section (to be discussed later).

6. Arrears Section

As well as rent arrears, the section deals with cases of default of mortgage payments to the Corporation. The emphasis is on exception reporting, since the section has no interest in the vast majority of tenants and mortgagees who pay promptly.

Binders, arranged in order of collection districts, hold copies of the rent sheets used by the door-to-door collectors. If the tenant gets behind with payments a "narrative" sheet is opened on him, and is filed in loose-leaf folders, again held in collection district order.

Defaulters on mortgage payments are identified by computer analysis of the accounts held by the Treasurer's Department. Once again, the details of their under-payment are transferred from the computer print-out to narrative sheets, and a box-file of these is held for each of the five housing sub-areas.

Organisation is by area teams, who each have an index relating streets to collecting district numbers: these are frequently needed in order to access the binders or narratives. Each area also maintains two or three ring binders containing details of cases where direct payment of rent is being made by the DHSS.

7. Rebates and Allowances Section (Figure 2)

This is the youngest of all the sections, responsible for administering rebates to municipal tenants and allowances to private tenants. Faced with an immediate and large rush of applications, the section implemented some semi-automated procedures: rebate details are calculated on programmable calculators, and stored on edge-punched cards.

In the rebates section, work is divided among four teams on the basis of the first letter of the applicant's surname. The only file of any size is a name-ordered Kardex file maintained on all applicants.

8. Visiting Section

The section acts as investigative arm for other sections. Each housing visitor is assigned to a small area of the city, and carries out all visits requested for that area. There is a standard form for each section making a request: the details sought on each form are summarised in Figure 6. The most commonly used form is the Visitor's Report Card, as used by

Applications and Overspill. In the case of a transfer application, similar assessments are made by the rent collector from the district concerned.

A visitor usually has to assess the suitability of the person visited, for old or new property. Apart from the difficulties of making any subjective assessment of this kind, the visit may well be to a house in which an applicant is living as a lodger. The visitor can then only make an informed guess as to how the person would treat accommodation of his or her own. It may also be the case that the applicant is sick or elderly, so that shortcomings in the standard of housekeeping may reflect this rather than an unwillingness to cope with more suitable accommodation. The problems of the visitor in these respects have been analysed elsewhere. (4)

The three most controversial items of information collected by visitors concern income, mental stability, and race. The statement of income is only for general guidance, and has become less significant since the widening of rebate eligibility. Nevertheless, discrepancies could show up between the figure reported by the visitor and those from other sources, and this appears to be the one item of information which people occasionally resent giving.

Any evidence of mental instability is of concern to the Corporation as a potential landlord, but distinguishing between eccentricities of manner and more seriously anti-social tendencies is likely to be difficult in one interview. Information in this regard needs to be tentative: a visitor may include a phrase such as "acted strangely" in the free form comments allowed for on the V.R.C.

The race of the applicant will be quite apparent to the visitor, and possibly unambiguous, but people's reservations here are more likely to centre on the part such information may play in decisions made about them. None of the visitor's forms includes any standard entry for race, but nevertheless some indication will usually be put on the form and is used in later decision-making. This is because of the Corporation's policy of dispersing the immigrant population so far as is possible among the complete range of its properties. Thus where the proportion of immigrants is already high, certain properties may be designated N/C - not coloured - on the central TV file. Sections such as Applications, Transfers and Re-housing must have an indication of race on their own files in order to be able to take cognizance of this.

9. Tenancy Queries Section

Though nominally subordinate to Lettings, the section has tended to develop an interesting role as a contact point with outside agencies, and as such, an advisory role vis-a-vis other sections.

The section invokes the help of housing visitors in two common instances - firstly, where a tenant has died and a lodger (usually a son or daughter) has stayed in occupation: and secondly where marriage breakdown has resulted in one or other of the spouses leaving home. Standard forms (A273 and A274) are used by the visitor to assess the current situation at the home. As well as these difficult cases, the section processes about 80 cases a week where a non-controversial amendment to files is required - eg., the death of a joint tenant.

Cases tend to be referred to Tenancy Queries by other sections encountering discrepancies in information given by clients, or other

indications that the situation may be irregular. A tiny minority of cases - about 3 or 4 a year - are initiated by anonymous letters from disgruntled neighbours or relatives.

As well as commissioning visits, the section may institute enquiries to the Rates Department, to establish who has been paying the rates: to the Department of Employment to see if N.I. stamps have been paid in regular work: or to the Public Health or Education Welfare Departments. Public Health may notify reciprocally if they come across a house owner concerned in smoke abatement procedures, who is also the tenant of a council house. A major source of information is the Bush House case file: from this it may be possible to deduce the length of residence of different occupants of a house.

The only pressure operating to the detriment of the client (and it is not suggested that it necessarily prevails in this case) is the element of "trading" of information which can arise in such a section. Its success rests on the ability to keep on good terms with other agencies. There can therefore be a temptation to provide information in the hope that at some stage other information may be forthcoming in return. The section appears to be conscious of this danger, and I was assured that the confidentiality interests of clients remains uppermost.

The Study

Method

The method of observations was adapted from that used in the social services office. However, because the work was more routine and clerical in nature, the opportunity was taken to assess the organisation and use of files in some detail.

A convenient and typical group was studied in each section: this would normally comprise four or five people. Their activities were logged, with particular note being made of each file access and telephone call. The use of letters and standard forms was often difficult to assess, as these would be processed in batches at irregular intervals.

Each group was studied for between 2 and 5 days. The decision to prolong study beyond 2 days depended on whether there were few or several main contact points outside the section, and whether the section regarded their work as very cyclical within a working week. The more contact points and the more cyclical the work, the longer the study. A total of 19 working days were observed.

From the sample figures, estimates were then made for each section as a whole. The multiplication factors used were as follows:

- (a) Applications. The 2-bed queue team (5 people in all) was studied for 5 days. The total staff at the time working on 1-bed queue, 3-bed queue, Homeless, and Housing Association cases was 17. Staffing therefore suggested a factor of 3.4, but since 5 sub-sections were involved, the factor was increase to 4.
- (b) Transfers. The section is divided into 5 area teams. A working week comprises 25 team-days. 3 team-days were studied, suggesting a factor of 8.
- (c) Re-housing. 9 staff-days were observed. A week would typically be 35 staff-days, giving a factor of 4.

- (d) Arrears. 2 area teams were studied for 5 days, giving a factor of $2\frac{1}{2}$ for all 5 teams.
- (e) Rebates. (Note: only the Rebates, as opposed to the Allowance, section was studied)

The section is divided into four teams; 3 team-days were studied, one of them covering calls via a telephone extension more generally used than others. The factor therefore was estimated at 6.

As with the social services study, the purpose of the observations was explained to everyone individually beforehand. In a working environment of this kind, there were bound to be suspicions that the observations were instituted by the management as work study.

Results.

Figures 6 and 7 summarise the data held in files and collected on standard forms. Figure 8 shows the incidence of telephone communication, with the weekly estimates derived in Figure 9. Also shown in Figure 9 (in brackets) are the calls which resulted in reference being made to one of the section's files, a process which is as close as administrators currently get to interrogating files other than their own, and which might be supplanted by on-line database interrogation.

Figures 10 and 11 show the main lines of communication to and from the sections studied.

Conclusions

As with social services, a large proportion of Bush House's incoming telephone calls are from clients (about two-thirds of the estimated weekly calls). Apart from its clients, Bush House has regular dealings with

comparatively few agencies, and even then it is more often a receiver rather than an initiator of enquiries. This suggests that Bush House is (in respect of the sections studied) a dispenser of information in the general sense described by Carroll et al in their study of Canadian institutions. (5)

It is possible to envisage three kinds of computer-based link between Bush House and outside agencies.

- (1) Social Services Department. About 60 calls per week (n) require reference to one or more of the files. The two main areas of enquiry were rent arrears and pending applications (see Figure 9). Direct interrogation of these files, as stored on a computer, might have attractions for S.S.D. workers, but their present enquiry rate would not justify the link in economic terms.
 - (2) Treasurer's Department. While the Arrears Section continue to act as an enforcement arm for mortgage payments, it could make good use of on-line access to the mortgage accounts. A more practical solution would probably be to combine the accounting and debt-collecting functions in one office. However, the situation provides an interesting example of a division of responsibilities, created for historical and political reasons, which results in personal information being duplicated and passed between departments in a way that is not
-
- (n) This is of course the only figure for which there could be any kind of cross-check. The figures for Area 9 were: to Bush House 20 calls; from Bush House 5 calls per week. Estimated calls from all social services offices to the Bush House sections studied were 125 per week, with 20 in the reverse direction.

strictly necessary. There may be situations where such a division of surveillance and control activities is desirable, but in this instance no gains accrue for anyone.

- (3) DHSS. The DHSS is concerned mainly with supplementary benefits cases, where rebates are payable by Bush House, or a tenant is falling behind with rent payments. The rate of contact would certainly appear higher if all Rebate and Allowance activities were included.

Unlike other sections, the Rebates section has a high rate of outgoing calls, mainly to DHSS. Often these are just to establish whether an applicant who has identified himself as being in receipt of supplementary benefit is in fact on the DHSS files: from this point standard procedures take over.

On-line access to DHSS files might therefore be sought in the long term, but a more imminent possibility would be the exchange of lists and accounts in machine-coded form for batch processing.

Within Bush House, three lines of development can be envisaged:

- (a) the computerisation of the property files, perhaps in conjunction with Public Health and Public Works;
- (b) the development of on-line tenants' accounts, to facilitate payment at different offices, and to allow instant arrears checks;
- (c) lettings files linked to the property files, so that the status of a property - particularly one believed to be vacant or on offer - could be established at any time.

Any of these developments would raise questions of the range of information to be merged. For example, for what activities is it relevant to have arrears information? If there are links to the property files, should any of these be available to other users of the property file, from other departments?

Finally, some conclusions can be drawn on the general issue of whether integrated systems offer attractions in avoiding duplication of information collection or storage. For example, it is sometimes argued that computer-based information systems will eliminate repeated form-filling by members of the public. The implication is that the citizen is being asked for the information because this is easier than retrieving it from the files of the organisation.

Only one instance of this could be found in the forms used by Bish House. On the Transfers/Exchange application form, the tenant is asked to give various details of his present accommodation. As a landlord, the Corporation already has this information.


Figure 6 also suggests that people may be asked repeatedly to give details of their families, and other dependents or lodgers. However, it can reasonably be argued that family sizes change - children are born, or leave home - and the gaps between form-filling may be quite long. The only exception is for people on rebate, who will have to confirm the details on their application form every half year. There might therefore be some attraction in combining the rebate and property files; much less further information would then be required for transfer or overspill applications.


6. Overall conclusions


A strong contrast with Social Services can be found in the attitudes of information collectors towards their clients. A social worker has to identify with the client, and often makes applications to other agencies on the client's behalf. But since the social services department has comparatively few financial or other tangible benefits to offer, little of the work is taken up with deciding on the relative merits of client' claims. This is, however, the essence of housing administration. The housing visitor, or the clerk who interviews someone coming to Bush House to discuss their case, cannot avoid the awareness of being part of an adjudication process. He will often have to point out that other people have stronger claims, or that certain housing is in short supply. The applicant will therefore be anxious that the details put on file are as favourable to him as possible. The clerical worker will see his main task as that of assessing information on all clients fairly. This gives rise to a quite different set of pressures when questions of confidentiality arise.


A major protection for the Bush House client is that information is collected and distributed by standard procedures in the main. If non-standard information is required, the matter will usually be referred to the Tenancy Queries section, whose members are very much alive to the confidentiality issue. However, the general reliance on standard procedures makes it all the more important that procedures designed round a computer system should be introduced with privacy in mind. Privacy protection will have to be presented to the clerical officers as part of a formalised, rather impersonal set of routines, and it is in this kind of environment that dependence on privacy labelling might be particularly appropriate.

FIGURES 1 - 5 KEY

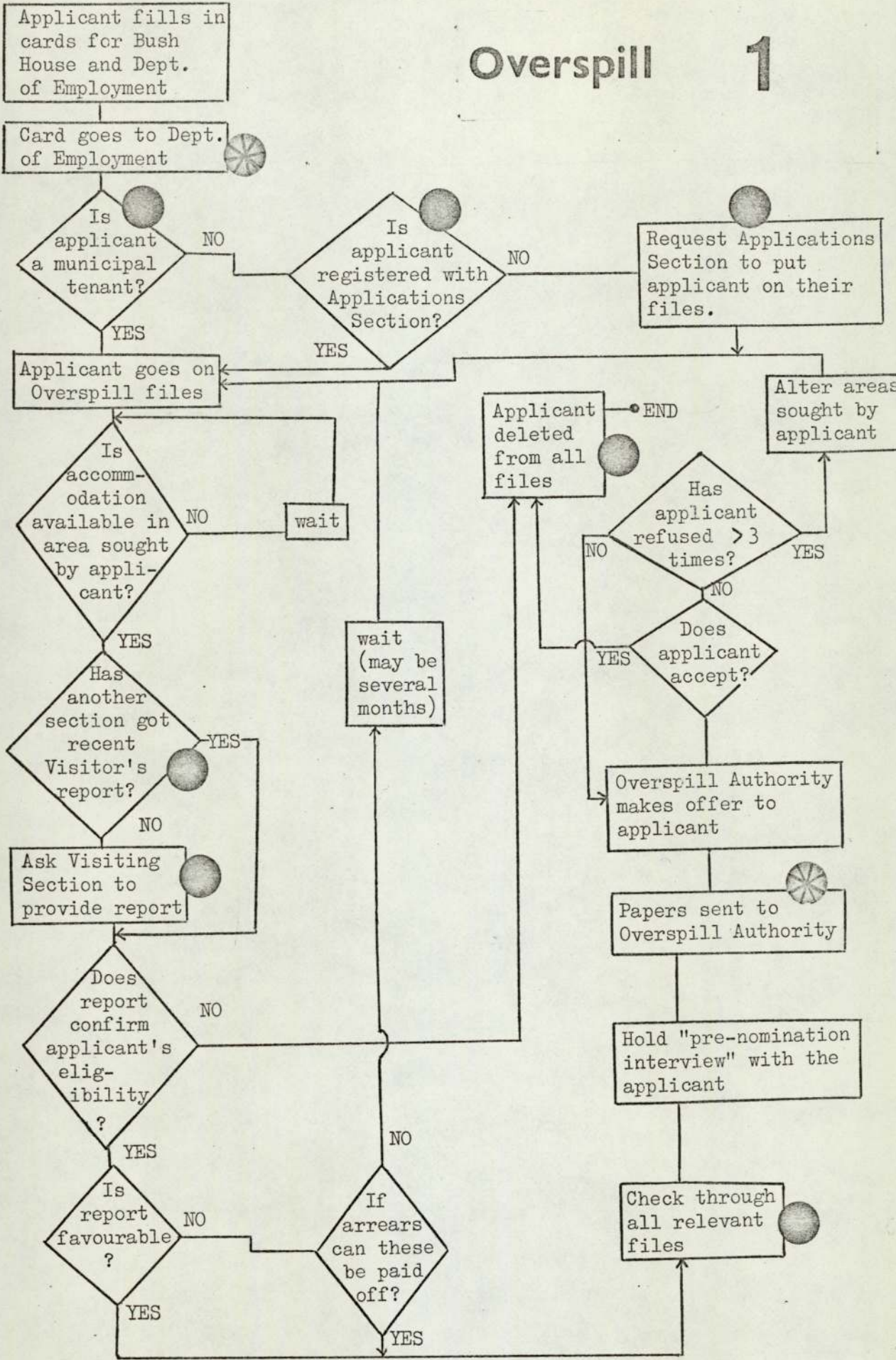
-  Denotes that the activity involves the section in providing or seeking personal information, with respect to another section within Bush House or another office of the Housing Department.

-  Denotes that information passes to or from another agency within Birmingham local authority.

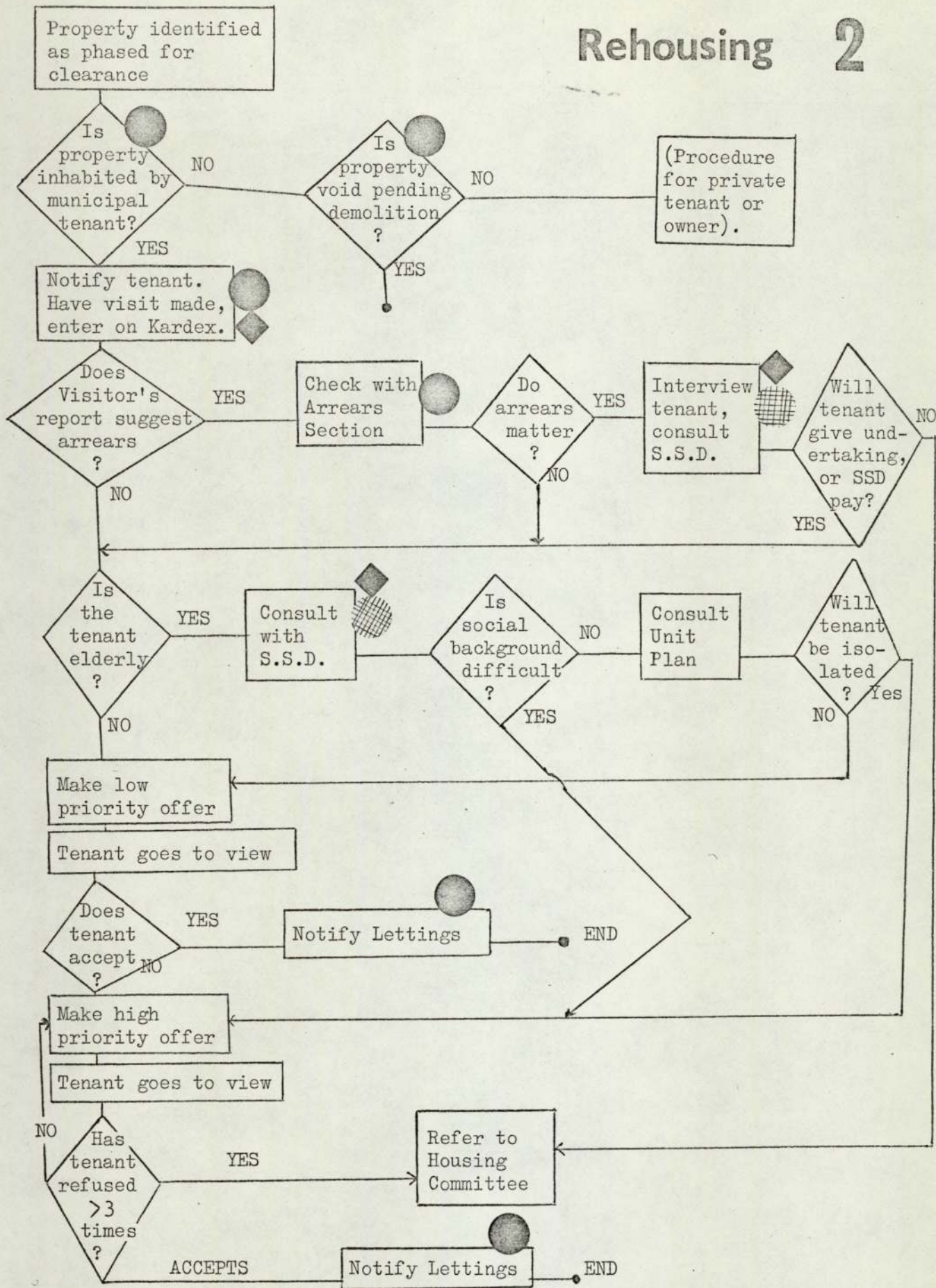
-  Denotes that information passes to or from an agency outside Birmingham local authority.

-  Denotes that the activity centres on a "collector" obtaining information (usually by a visit or on a form) for the first time in a particular information-chain.

Overspill 1

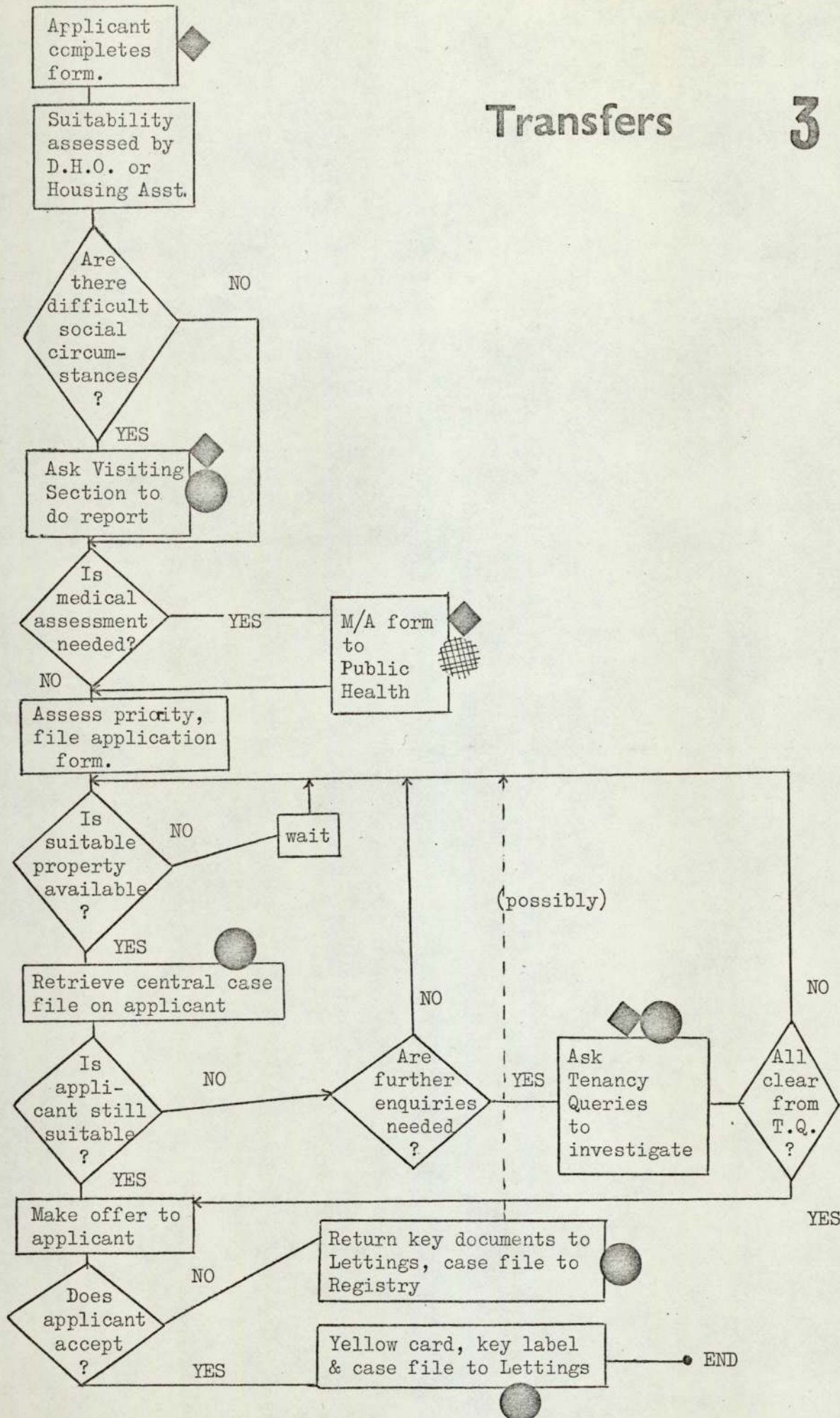


Rehousing 2

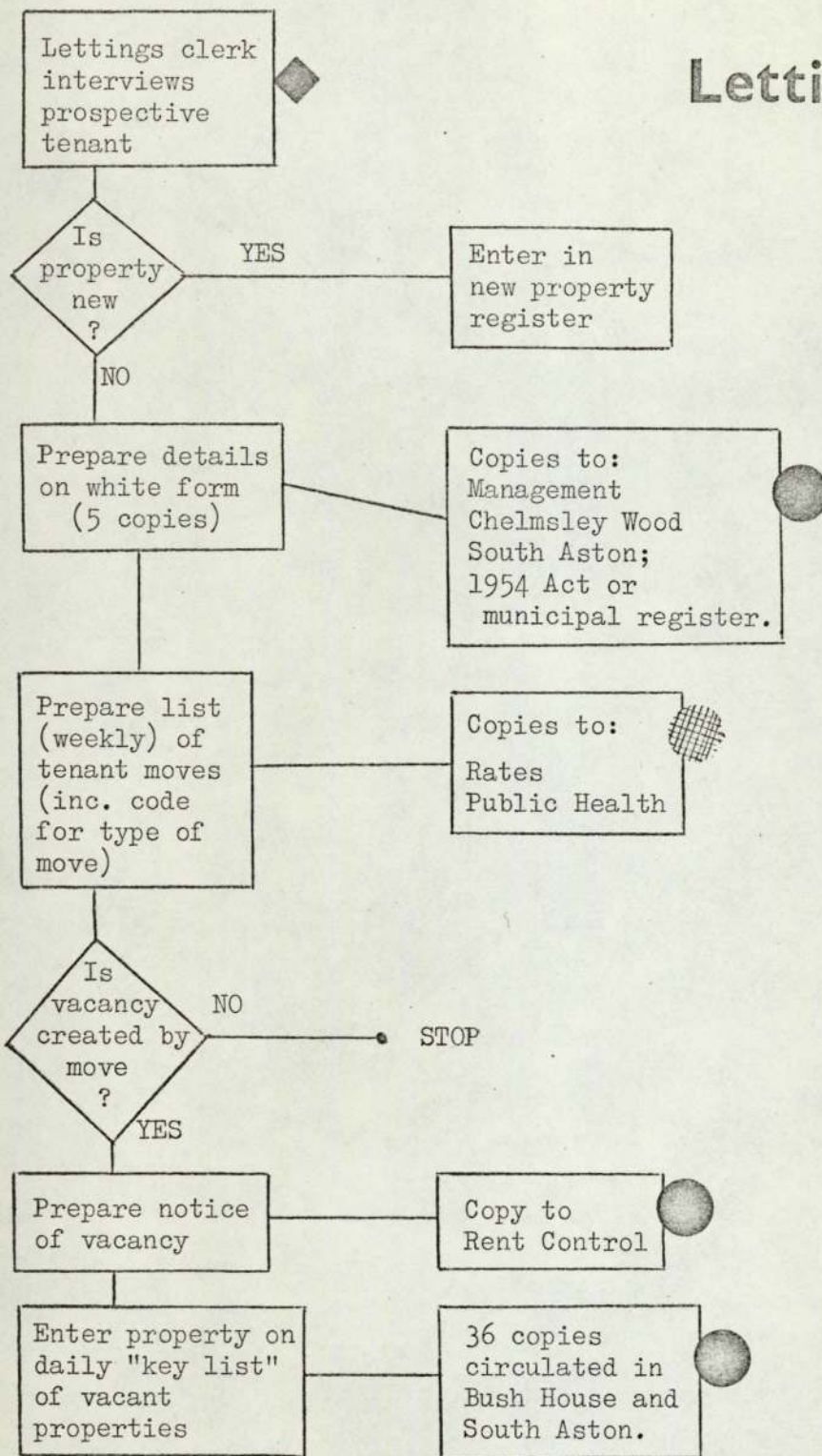


Transfers

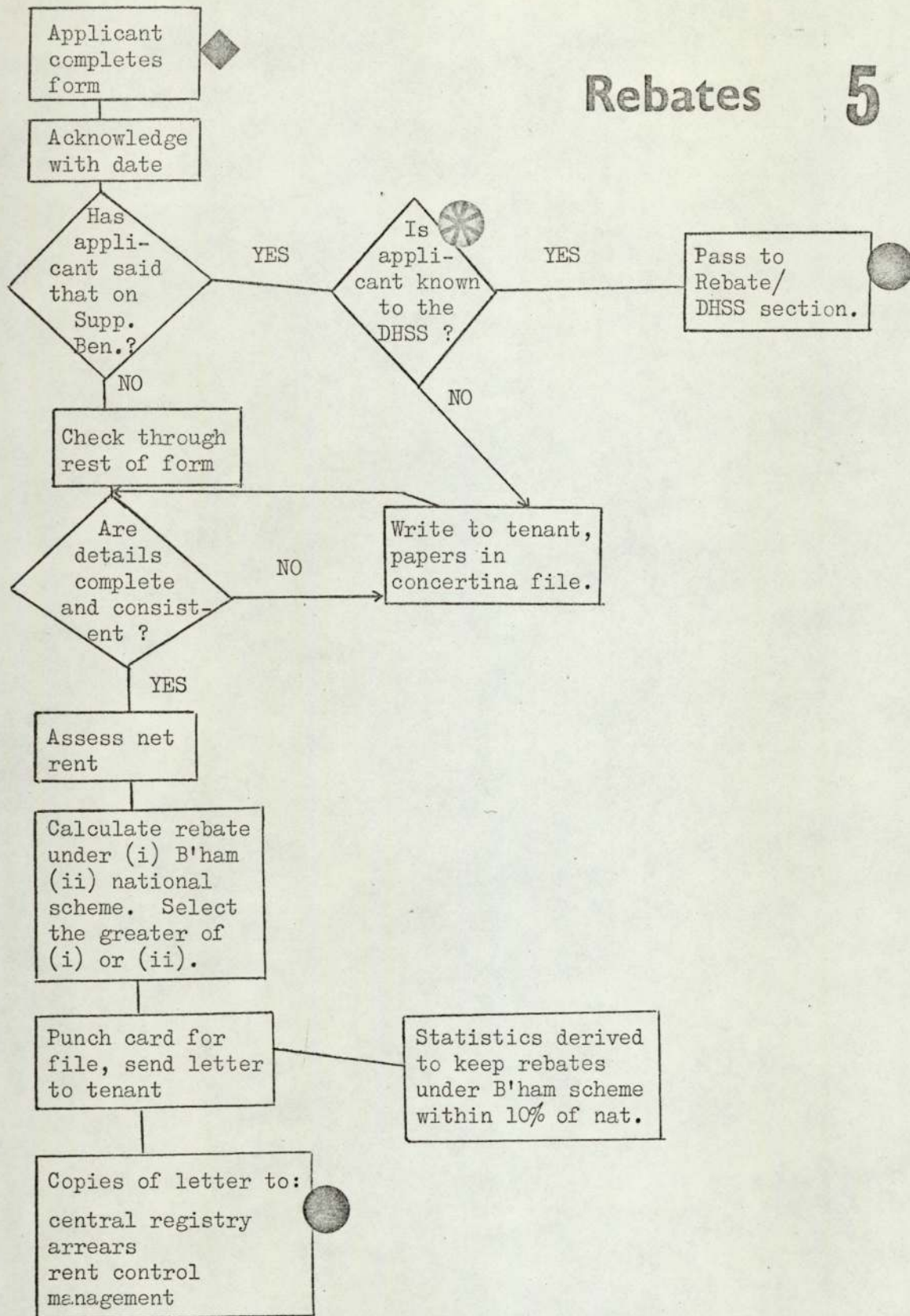
3



Lettings 4



Rebates 5



FORMS USED
BY BUSH
HOUSE SECTIONS

VISITORS' REPORTS						APPLICATION TO				MUNICIPAL TENANTS ONLY?		
LODGER	T.O. (A273)	T.O. (A274) MATRIMONIAL	1954 ACT: RE-VISIT	HOUSE SALE	SITE CLEARANCE	V.R.C.	REBATE	OVERSPILL	TRANSFERS			APPLICATIONS
YES	YES	NO	NO	NO	NO	NO	YES	NO	YES	NO		
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	NAME	IDENTIFYING DATA
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	ADDRESS	
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	REGISTR'N NO.	
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	AGE OR D.O.B.	PRESENT ACCOMMODATION
<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	LENGTH RESIDED	
<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	RENT	
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	SANITATION	
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	NO., TYPE OF ROOMS	
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	STANDARD OF HOUSEKEEPING	HUSBAND'S -
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	LODGER?	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	INCOME	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	JOB	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	EMPLOYER	WIFE'S -
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	HEALTH	
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	AGE OR D.O.B.	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	INCOME	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	JOB	CHILDREN
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	EMPLOYER	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	HEALTH	
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	NUMBER	
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	AGE OR D.O.B.	FREE-FORM COMMENTS?
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	HEALTH	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	SCHOOL	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	YES	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	YES	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	YES	

= STANDARD ENTRY = OPTIONAL OR IN CERTAIN CIRCUMSTANCES

Figure 6

	By SECTION, AREA OR WITHIN SECTION?	FILE NAME	TYPE OF FILE	MAIN IDENTIFIER	MAIN CONTENTS	NO. OF INDIDS (APPROX)	INDIDS ON FILE
	S	STREET-INDEXED	CARD TRAYS	ADDRESS	NAME, REGISTRATION NO.	14,000	Eligible applicants
Applications	S	CASE FILES	FOLDERS	NAME	ALL DOCUMENTS FROM PROCESSING APPLICATION	14,000	Eligible applicants
	S	REGISTERED OF ENQUIRIES	CARD TRAYS	NAME	DATE WHEN ELIGIBLE	11,600	Non-eligible applct's
	S	V.R.C.'S	KARDEX	NAME	STANDARD V.R.C.		Eligible applicants
Overspill	S	APPLICANTS	CARD TRAYS	NAME	AREA WANTED, REPORTS	< 1,400	Overspill applicants
Re-housing	S	UNIT PLANS	MAPS IN DRAWERS	UNIT NUMBER	LOCATION OF PROPERTIES PHASED FOR CLEARANCE		People living in clearance areas
	A	TENANTS	KARDEX	NAME	VISITOR'S REPORT	< 3,000	People living in clearance areas
Transfers	A	STREET-INDEXED	CARD TRAYS	ADDRESS	TENANT'S BED QUEUE AND PRIORITY		Transfer applicants
	A	TENANTS	CARD TRAYS	BED QUEUE / PRIORITY	SUITABILITY, PROPERTY WANTED BY TENANT		Transfer applicants
Slum Clearance	S	PROPERTY FILE	FOLDERS	OWN NUMBER SYSTEM	DETAILS OF OWNERSHIP		Owners of property liable to C.P.O.
	S	COLLECTORS' SHEETS	BINDERS	COLLECTION DISTRICT	PAYMENT HISTORY (≤ 2 YRS)	90,000	All Bush Hse tenants
Arrears	S	NARRATIVES	FOLDERS	COLLECTION DISTRICT	CURRENT ARREARS POSITION		Tenants in arrears
	A	MORTGAGE ARREARS	PLASTIC WALLETS	ACCOUNT NUMBER	CURRENT ARREARS POSITION	< 1,000	Mortgagees in arrears
Rebates	A	DHSS	RING BINDER	NAME	RENT PAYABLE DIRECTLY BY DHSS		Tenants on direct payment
	S	REBATES	KARDEX	NAME	INCOME, FAMILY DATA	24,000	Rebate recipients

Figure 7

SECTION AND FRACTION OF SECTION-WEEK STUDIES.												Total		
	CLIENTS	INTERNAL (GUSH HOUSE)	SOUTH ASTON / CHELSEA WOOD	TREASUR. OR TOWN CLERK	PROBATION	SOCIAL SERVICES	DHSS	PUBLIC HEALTH	NHS	VOLUNTARY ORGANISATIONS	EMPLOYER		OTHER	
APPLICATIONS	2	142	10	7	1	2	13	2	3	6	2			188
	1/4	2	3	3					1				1	10
TRANSFERS	2	57	9			2				2			1	71
	1/8		5	2						1			1	9
RE-HOUSING	2	38	32	4		4				1	1			80
	1/4		10			1								11
ARREARS	2	76	35	2	2	1	18	11		2	8	1	3	159
	2/5	2	27	3	2	2	8	10		1	2	2	3	62
REGATE	2	16	4					13						33
	1/6		11					20				9		40

Telephone calls: source figures

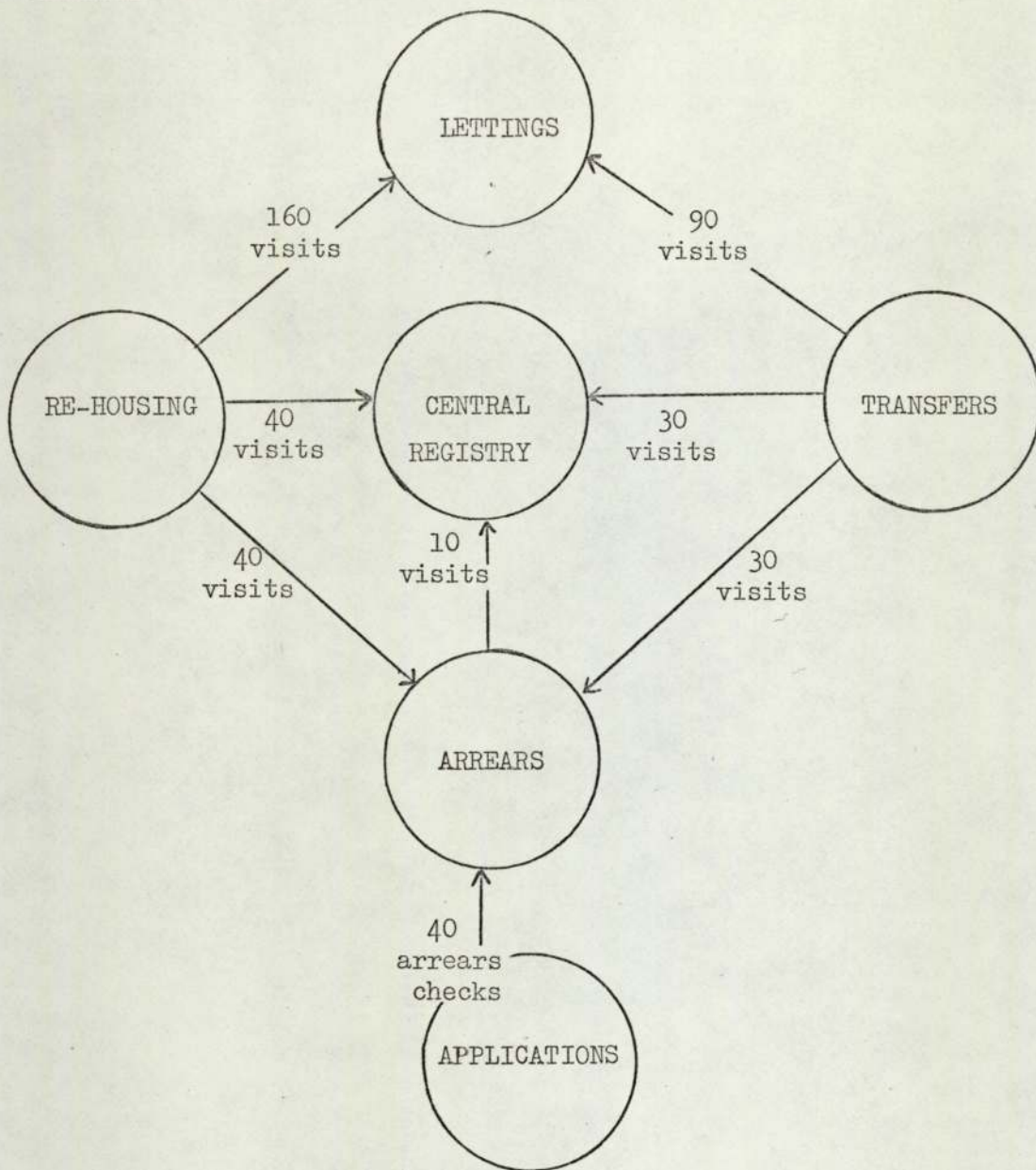
Figure 8

SECTION								
	CLIENTS	BUSH HOUSE	SOUTH ASTON, CHELSEA, WOOD	SOCIAL SERVICES	DHSS	PUBLIC HEALTH	NHS	OTHER
APPLICATIONS	570 (200)	40 (15)	30 (10)	50 (30)	10	10 (5)	25 (20)	
	10							
TRANSFERS	390 (175)	70		15 (5)			15 (5)	
	40		15					
RE-HOUSING	150 (60)	130 (45)	15	15 (5)				
ARREARS	190 (55)	90 (25)		45 (20)	30 (15)			15 (voluntary associations)
		70		20	25			
REBATES	100 (10)	25 (5)			80 (10)			
	65				120			50 (EMPLOYERS)

Telephone calls: adjusted to give estimates for one section-week. Figures of less than 10 have been disregarded. Figures in brackets denote calls requiring reference to one or more files (figures of less than 5 disregarded).

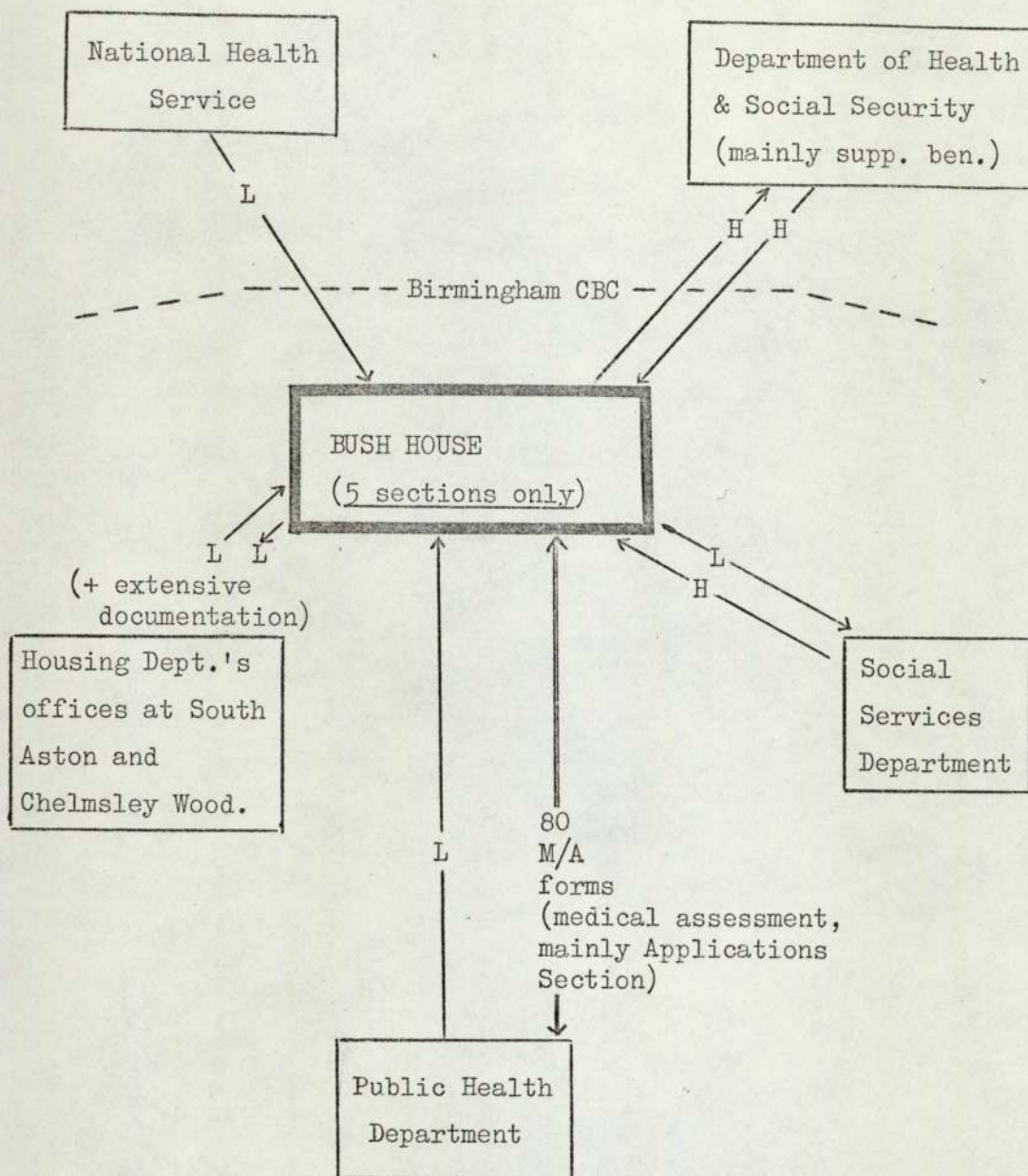
Figure 9

Communications: within Bush House.



Based on estimated figures for one week.

Communications: Bush House to outside agencies.



Based on telephone calls, figure 9, ante.

H indicates more than 100 p.w., L between 10 and 50.

CHAPTER 8EDUCATION1. Introduction

The compilation of records on children has already been discussed in connection with the Social Services Department (ant, chapter 6), but in that case only a minority of children were likely to be affected. In the case of local authority schools and colleges, the great majority of children will have files compiled on them. At present, most of these files are kept by and within the various educational institutions. However, as time goes on, computerisation may lead to a particularly marked centralisation of records for some aspects of educational administration. Not only will all the questions of the proper control of dissemination of current information then arise, but there will be ticklish questions as to how long records should be retained. If, for example, a child plays truant from school, might this be seized on later as evidence of unreliability? If a technical college student organises a sit-in, could this haunt his later career?

The feeling that young people should be able to make mistakes, and perhaps even a few enemies, in any education having a proper element of inquiry and adventure in it, was very evident in the Gallagher hearings in the U.S.A. (a) Indeed it is hard to imagine any education which could be more stultifying than one where the student sensed that every activity would be documented and used in assessments at some indeterminate point in the future.

(a) See Appendix I. The 1965 hearings concentrated on psychological tests, including their use in schools; and the 1966 hearings included discussion of lecturers' assessment of students (see eg., the testimony of C.A. Reich).

2. Legal background

A local education authority is obliged to provide schools, (b) but the duty to ensure attendance is the parents'. (c) Prosecutions for failure to ensure attendance are to be brought by the authority, (d) which will usually be served by Education Welfare Officers, who investigate the reasons for non-attendance and encourage compliance by less formal means. In order to enable the E.W.O's to keep files on the whereabouts of children coming up to school age, the authority is entitled to details of births from the local Registrar. (e)

A local education authority will also usually exercise its option to run a Youth Employment Service, (f) and if so the transfer of information from the schools to the Y.E.S. is governed by regulations. (g) These limit access to the information to Y.E.S. officers, Inspectors of Schools, and others authorised in writing by the Minister. (h) All records must be destroyed when the child reaches the age of 21. (i) Records must relate only to health, ability, and educational attainment and aptitude, insofar as these relate to future employment. (j) A parent or guardian may inspect the record in the presence of the Y.E.S. Officer responsible for it, but they may not take copies. (k)

(b) Education Act, 1944, s.8.

(c) Ibid, s.39

(d) Ibid, s.37 and 40 (2) as amended

(e) Ibid, s.94 (2)

(f) Employment and Training Act, 1948, s.10

(g) Youth Employment Service (Particulars) Regulations, SI 1948/1118

(h) ie., Minister for Employment. Ibid reg.4

(i) Ibid, reg.5

(j) Employment and Training Act, 1948, s.13 (2)

(k) Ibid, s.13 (3)

The local education authority may make grants to the parents of school pupils, (m) and to post-secondary students. (n) Grants must be given for students enrolled on full-time first degree courses. (o)

Besides educational responsibilities, the local authority is under a duty to provide for medical inspections of school pupils, (p) and may inspect for, and take measures to ensure, personal cleanliness. (q)

3. Record-keeping: the Birmingham L.E.A.

3.1. Files. The broadest centralised file is that maintained by the Education Welfare Department. Even this file, which covers about 170,000 children, comprises only single cards for each family, giving the names of the parents, the address, and the dates of birth of all the children in the family. A code for race is also included. If any steps have to be taken to ensure attendance these are entered on the card, but in many cases the card may not be updated once the youngest child has started school.

At the F.E. level, enrolment forms have been standardised among the city's technical colleges, and a scheme for computer processing of these has been under way since 1969. The aim of the scheme is to facilitate accounting (since a lot of debiting to employers and other local authorities is involved), and to compile statistics for the D.E.S. The records are

-
- (m) Education Act, 1944, s.81
 - (n) Education Act, 1962, s.2.
 - (o) Ibid, s.1
 - (p) Education Act, 1944, s.48
 - (q) Ibid, s.54

limited to name, date and country of birth, address, address of employer, course details, and educational history. 125 words (24-bit) are allowed for each record.

Otherwise, the way in which files are kept is a matter for the discretion of each educational institution. In one school, (r) progress reports are kept in folders in a locked cabinet in the Headmaster's Office. Some folders contain information in sealed envelopes marked "to be opened by Headmaster only". When a child leaves this particular school he is provided with a report on a two-page standard form. This contains two sections marked "confidential", and statements to the effect that further confidential details can be obtained from the Headmaster.

At one of the city's technical colleges, (s) on the other hand, record-keeping is devolved more to heads of departments. Because of the standard enrolment forms, mentioned earlier, and the need to cater for mainly part-time students, more administrative data has to be recorded, but there is rather less scope or requirement for character assessment by the teachers.

3.2. Forms. Standard procedures exist for transferring and collecting personal information, in the following instances.

3.2.1. child guidance clinic. A child may be referred to the clinic by means of an "application form" on which only three lines are provided for stating the "nature of the problem"; a report will usually be sought from the head teacher on a form headed "confidential", in which comments are

(r) Perry Common Comprehensive. Visit of 18th March 1971

(s) Brooklyn Technical College. Visit of 12th January 1973

given on the child's home background, and behaviour at school.

3.2.2. Youth employment service. Birmingham operates its own service under a Scheme of 1964. A standard form goes to the Y.E.S. for each school leaver. If a child leaves school at the earliest permissible age, the report (Y.15) comprises details of attendance, health, aptitudes, and skills, in accordance with the legal requirements (section 2, ante). A modified version of the form is used for children from special schools. Notes are provided to explain the standards to be adopted in making some of the assessments.

A different form for older school leavers (Y.18) invites a few additional comments on character (such as "promise of displaying initiative"), reflecting the more predominantly white-collar employment market aimed for by the late school leaver.

3.2.3. educational awards. A number of forms are used for applicants for grants at secondary, F.E. and H.E. levels. Some of the forms are headed "Strictly Confidential", others just "Confidential". For dependent students, a parent will have to provide details of all his dependent children, major expenses, and income from all sources. He will have to obtain a certificate of income from his employer, and the forms for this (t) show some interesting variations: for school awards, the form is headed "Strictly Confidential", and "Maintenance Allowances ... Information required in connection with an application for an award under the Authority's Scheme"; for teacher training the form has no "Confidential" heading, but the purpose of the declaration is clearly explained; for university grants, the form

(t) All versions of "Form 20". (The application forms are all coded 19)

has neither a "confidential" heading, nor an explanation of the purpose of the form.

4. Data furnished to the Department of Education and Science

A local education authority is required to generate extensive statistics on its activities for the national government. Much of the information is provided in anonymous tables. However, some returns are for samples of the student population, for which a considerable level of detail is sought.

For example, one in ten F.E. students may be asked to fill in, by name, Form 160 or Form 161. These forms comprise questions on employer, course and educational history, which are very similar in character to those on Birmingham's F.E. enrolment form. However, the D.E.S. forms have a very explicit heading, stating that access to the information will not be given to anyone outside the Statistics and Computer Divisions of the D.E.S., without the consent of the student.

Another F.E. form (Form 113) seeks information on GCE "A" level results for one in five students. The information again includes the student's name, but is intended for completion by the educational institution. No guarantee of confidentiality is given. Apart from the "A" level details, the form seeks name, age, date of birth, and course category of the student.

The insistence on obtaining full identifying data on each student reveals the interest of the D.E.S. in being able to plot the progress of particular individuals. Since selection for inclusion in the samples is by the day of the month on which the student was born (u) a consistent fraction of the population is selected. Plans have been developed by the

(u) ie., 5th, 10th ... 30th for 1 in 5, and 5th, 15th, 25th for 1 in 10

D.E.S. for keeping files at the Department's Darlington computer centre, such that individual's progress could be followed through all the major types of educational institution.

5. Computer based systems: the future

The most likely areas for early computerisation are the basic details of achievement and attendance, and school medical data. Schools in Memphis, USA, already record tests and attendances using punched cards sent to a city computer centre, (1) and audio response units capable of sending this data through the telephone network have been used in one school district in Michigan. (2) In this country, Gloucestershire County Council has computerised school medical records, including entries with clear privacy implications (eg., history of bedwetting). (3)

A computer can of course also be used as a teaching aid, as in the Chicago scheme for remedial teaching of reading and arithmetic. (4) With these prospects for using a centralised system for giving instruction (and thereby logging performance): for marking tests (whether intellectual or psychological); and for storing dossiers on every child, it seems that the accumulation of data in one centre could be substantial. The Memphis data processing director already envisages the introduction of computer-aided instruction, and the expansion of individual dossiers to 3000/5000 characters. (5)

In the longer term, education planners might seek to relate their data to other records in a computerised local authority system, in order to forecast the demand for different kinds of educational provision. They might hope to unravel much more easily the kind of statistics which had to be collected laboriously for the Newsom Committee in 1961, (6) concerning

the achievement, curricula, attendance and home background of schoolchildren. At a more individual level, research is already proceeding into the possibilities of using computer matching between school-leavers and would-be employers. (7)

6. Conclusions

As with Social Services, Education is served by a body of people having a separate professional identity, and direct involvement with their clients. However, teachers are in a more powerful position with respect to their pupils, particularly where the child has any ambition to take up a career based on academic achievement. While teachers' observations remain on files in the various institutions, their origins and authorship will tend to be familiar to anyone basing decisions on them. But if these observations should be coded for machine processing (or perhaps turned into "measurements" of a rather contentious kind) then the preservation of sufficient context-data could become a very important matter.

A number of dangers arising from computerising educational records have been instanced by Ramey, (8) but his particular fears are not shared by this author. Ramey's basic thesis seems to be that integration of educational and other records could prejudice the chances of children from deprived homes, since they would be unable to "live down" their under-privileged backgrounds. An opposite argument would be that discrimination can be more effectively exercised through the traditional procedures of interviews and references, rather than computer based selection. However, the computer could well become central to a new form of this prickly political debate, which has been simmering on, in both educational and broader terms, for some time.

Returning to the present, the problems of restriction of access to information most commonly arise when a student or pupil is in trouble. Trouble at school is often just one outcome of a troubled and confused situation at home. Thus it is very difficult to lay down general rules about disclosure to people such as social workers, police, or even other members of the family. A technical college principal, for example, instanced a student who was at risk of physical assault if located by certain members of her family, so that her address had to be treated as highly confidential. This provides an interesting example of the capability of almost any data to be "sensitive" in a particular set of circumstances.

Teachers have responsibilities both to the parent and the child, and confidentiality may be owed to just one or both of the parties. Especially with older children, it may be difficult to decide whether parents should be informed if a child confides in a teacher about a sensitive matter. A child may also want to conceal matters from other pupils (visits to a child guidance clinic may be arranged out of school hours for this reason). Normally these situations can be covered by good sense in the personal relationships formed by the teacher, but a lot could go awry if centralised records made it easier for administrators far removed from the situation to establish that the child was, for example, attending a clinic for contraceptive advice or child guidance. Such information would not have to be revealed directly - for example, someone basing routine procedures on the contents of the central file might order a follow-up visit by a health officer or social worker, thus spilling the beans by implication to anyone at the home address of the child.

Thus in the educational field it can be concluded that ethical decisions on privacy may be difficult, although limited in the main to a small minority of cases; the pragmatic privacy considerations are waiting for us in the long-term future, but, given the roles that the computer may one day play as teacher, examiner, and record-keeper, these considerations may become extremely controversial.

CHAPTER 9RATING AND FINANCE1. Introduction

Accounting is one area in which local government computing is already fairly well advanced. However, much of this work relates to goods and services, rather than records on individual citizens.

The financial records on individuals which a local authority is most likely to hold concern rate payments, council mortgages, and the staff payroll (which may be quite substantial -- about 56,000 people are employed by Birmingham Corporation). Other departments, particularly Housing, maintain accounts on individuals, and there may be a certain amount of information exchange: for example, council house tenants usually pay their rent and rates together, and the housing department has to separate out and hand over the rates income.

Given that English people are fairly secretive about their income (whereas the Norwegians and Swedes treat it as a matter of public record), and may be even more secretive about other financial matters, there is no doubt that individual accounts need to be treated as private. Not so much because the information may be evaluative (as in "suitability" for a house, or a teacher's report), but because it carries authority. The wish to give an impression of earning more than you actually do, or of having rather less than the cavernous mortgage debt that you actually have, may be on the borderline of privacy, but access to the exact figures will be resented nevertheless.

Other considerations also apply. Where accounts reveal a bad payment record, the indid may wish to impose restrictions on the kind of people who should learn of this. This has to be weighed against the conflicting interest of another agency - perhaps some other department of the same authority - to assess the risk it is taking in allowing credit.

Finally, financial data offers an interesting example of the inter-relation of privacy and purpose of use. Particularly where details of income are volunteered by the indid, substantially similar data may have to be treated as being quite distinct for privacy purposes, because of the different circumstances under which different versions were acquired.

2. Legal background

Rating in particular attracts litigation, because people naturally wish to contest paying when they feel that the assessment has been less than fair. The assessment may be contested on the grounds of the valuation, or because of conclusions reached about the identity of the occupier liable to pay the rates. Valuation is not a local authority function, but the process of valuation will be discussed briefly, since it provides a useful example of conflicts between individual privacy and officialdom's need to know. The valuation list, which is passed to the local authority, and which must be available for public inspection, (a) may reveal a limited amount of information about the occupier, with regard to the use and value of his property, but is unlikely to offer any real threat to privacy. A more controversial issue is the duty of a local authority (as rating authority) to notify the valuation officer if any information comes to its notice which suggests that revaluation of a hereditament is needed:(b) this may be seen

(a) General Rate Act, 1967, s.108

(b) Ibid, s.85

as improper surveillance if, for example, the information is derived from planning approval given for an extension to the hereditament.

2.1. Valuation. Valuation has given rise to argument about the intrusiveness of official investigation. On a number of occasions prior to 1948, when valuation was still a local responsibility, the Courts upheld the right to resist intrusive questioning. Tenants of public houses successfully challenged demands for information about their business takings, (c) and in one such case, Cartwright v Sculcoates Union, (d) the House of Lords verged on basing its findings on a right of privacy. "There is nothing that a tradesman so much dislikes" commented Lord MacNaghten, "as any inquiry into his profits". (e) Lord Morris agreed that such information should be disclosed only if the tenant wished it, adding, unnecessarily one hopes, that inquisitorial force would not be brought to bear. (f) Lord Shand upheld the right of tenants to object to supplying evidence which would "... rip up affairs which they are not bound to disclose to the public". (g) In Grant v Knaresborough UDC, (h) the plaintiff successfully sought a declaration that a form purportedly seeking information required under the 1925 Rating and Valuation Act was in fact ultra vires, including questions on gross takings and outgoings over the previous three years. The judge described the form as "gravely oppressive". (i)

(c) Dodds v Assessment Committee of the Poor Law Union of South Shields

[1895] 2 Q.B. 133

(d) [1900] A.C. 150

(e) Ibid at p.153

(f) Ibid at p.155

(g) Ibid at p.156

(h) [1928] L Ch 310

(i) Ibid at p.317

However, judicial attitudes seem to have shifted with the more recent case of Watney Mann Ltd v Langley. (j) Much of the judgment of Thompson J. was taken up with the meaning of "such particulars as may reasonably be required" for compiling an accurate valuation list, from the Local Government Act, 1948. (k) As in Grant, the valuation officer had sought information about a pub's trade, and he argued that "reasonably required" ought to have a meaning along the lines of "the minimum needed" for assessment. The plaintiff on the other hand, claimed a more over-riding test of reasonableness. The learned judge accepted the defendant's construction, and held that the test was whether or not a valuation officer could compile an accurate list without the information: in deciding this he was prepared to consider the record and experience of the valuation officer concerned. (m) He was therefore interpreting a statutory protection against intrusive data demand on the basis of administrative needs rather than on the boundaries of a citizen's privacy. A similar, utilitarian, approach was taken with regard to the plaintiff's concern that information they revealed might be brought in as evidence in later proceedings: "The questions that arise are: (a) Is it a serious risk likely to be of frequent occurrence so as to outweigh as a disadvantage the advantage afforded by having the particulars? (b) Is it a risk that I should infer Parliament would not have suffered to exist if it had realised the possibility of its existence?" (n)

Both questions the learned judge answered negatively. He did not pursue the question of how one should weigh the disadvantage of the

(j) [1963] 3 All E.R. 967

(k) s.58 (1); (now s.82 (1) of the General Rate Act, 1967)

(m) Ref (j) at p.980

(n) Ref (j) at p.982

individual against the advantage of the administration. It may be argued that having rejected the over-riding test of "reasonableness", there was no need to consider such wider questions of balance of interest. However, such an approach is markedly different from the more generalised one of their Lordships in Cartwright, where, for example, Lord MacNaghten was all for treating the matter as one for "commonsense".(o) The second question suggests a freedom of interpretation which the courts do not have. Denning L.J. once referred to the need for the courts to "fill in the gaps" in legislation, and this was subjected to adverse comment in the House of Lords. (p)

It will be difficult, to say the least, for any judge to construe legislation of this kind as embodying Parliament's wish that privacy should be respected.

To emphasize the quandary which a valuation officer may find himself in, it should be noted that he may come under fire for not being inquisitive enough. In making a valuation, he may have to decide whether "substantially the whole of the available accommodation" is used by guests. (q) In Bickley v Tudge (V.O.), (r) a house had 9 bedrooms, and the family squashed into 3 of them during the summer season. In finding that the premises should be rated as a boarding house, the Lands Tribunal Chairman commented:

(o) [1900] A.C. at p.153

(p) See Lord Simonds in Magor and St. Mellons RDC v Newport Corporation [1952] A.C. 189, at p.190

(q) General Rate Act, 1967, Schedule 13, para 2 (1). The case which follows was based on the identical wording of s.3 of the Valuation for Rating Act, 1953.

(r) 1958 R.R.C. 24

"The appellant ... displayed some resentment that other similar properties escaped assessment as boarding houses, and I can well believe that more intimate knowledge of the circumstances than is available to the valuation officer may justify a feeling that there has been some unfair discrimination. However, it must be difficult for a valuation officer and his staff to find out what is going on behind closed doors; and all that can be done is to deal with each case as the facts come to light". (s)

2.2. Occupation. Liability to pay rates rests on the occupier of the hereditament.(t) A rating authority therefore faces decisions as to who to press for payment when this is not forthcoming. Demands may be addressed simply to "the occupier", (u) but if this produces no result, further investigation is needed. To pursue a claim for rates by distress, (v) the authority must establish actual occupation, exclusive occupation for the purposes of the possessor, possession having some benefit or value, and possession over more than a transitory period of time. (w) This means investigating the circumstances and relationships of people believed to have occupied the hereditament. The rating department may compile its own information on these points, or might wish to access information obtained by other departments of the authority.

(s) Ibid at p.26

(t) General Rate Act, 1967, s.16. The owner can be rated in some circumstances - s.55

(u) Ibid at s.109 (2)

(v) Ibid at Part VI

(w) Laing & Son Ltd v Kingswood Assessment Committee [1949] 1 All E.R. 224 at p.227

A recurrent privacy-risk situation occurs when a husband and wife separate. Typically, proceedings for divorce are started but are not yet completed. The husband moves to another house leaving his family in occupation, and sends them money voluntarily or under the terms of an agreement. Normally the husband will be taken to have retained "beneficial occupation" because of the availability of the house for sheltering his family. However, the rating authority will have to weigh up questions such as:

- (i) can distress for payment be sought against the wife as joint occupier? (probably not.) (x) But if the wife has a separate interest in the property or "this is not a case of allowing the wife to stay in the matrimonial home; the appellant has done his level best to get her to go", (y) then the wife may be liable.
- (ii) at what stage are the divorce proceedings" (Once a decree absolute has been granted, the husband ceases to be liable. (z)

In these and other circumstances where the liability of the husband is in question (eg., through mental illness, (a)) the authority has to investigate personal matters, at a time when they are most sorely felt.

-
- (x) Malden and Coombe Corporation v Bennett [1963] 2 All E.R. 527
- (y) Lord Parker C.J. in Des Salles d'Epinoix v Kensington & Chelsea LBC [1970] 1 WLR 179 at 182
- (z) Mourton v London Borough of Hounslow [1970] 2 All E.R. 564
- (a) Robinson v Taylor [1948] 1 K.B. 562

From the point of view of integrating files, it has to be noted that although a tenant is usually liable (as occupier) for rates, it is possible to be a "lodger" for rating purposes and a "tenant" for the purposes of other legislation (such as the Rent Acts). (b) Introducing a standard definition for "tenant" or "occupier" in the corporate database would therefore run up against the difficulty that the law itself does not attribute hard and fast meanings to these words.

2.3. Rate rebates. Rate rebate schemes are currently governed by s.49 and Schedule 9 of the General Rate Act, 1967. The calculation of rebates is on a quite different basis from rent rebates and allowances (for example, income is assessed over 6 months instead of four weeks or two months), and a Green Paper published in 1971 suggested reform of rate rebate schemes, adding: "There would clearly be advantages in aligning the details as far as possible with the new rent rebate proposals." (c)

Reform along these lines is now envisaged by Part II of the 1973 Local Government Bill. If this measure is enacted, the way will be clear for applications for rent and rate rebates to be based on the same application form.

As with rent rebates, the local authority is obliged to collaborate with the DHSS in respect of people receiving social security benefits. (d)

-
- (b) Helman v Horsham and Worthing Assessment Committee [1949] 1 All E.R. 776, particularly Lord Denning at p.786
- (c) The Future Shape of Local Government Finance, Cmnd 4741, at para 3.2.2.
- (d) Particularly under s.16 (2) of the Ministry of Social Security Act, 1966

Rationalisation of definitions still has a long way to go in this case: queries to the professional journals have included a war widow receiving an increment on her pension for a fifteen-year old daughter. Was the child a dependent for rate rebate purposes? (e) If a wife receives the cost of the rates from her husband, does this count as "income"? (f)

3. Rating accounts in Birmingham CBC

The following description relates to the procedures implemented on Birmingham's ICL 1904 machine. The accounts are currently being moved to a new 1906A system.

Birmingham's 400,000 rating accounts are filed, first, by some 5,000 street references, each hereditament then having (i) a property record of up to 58 words and (ii) an account record of up to 221 words. The first record includes data from the valuation made by the Inland Revenue. The second gives a comprehensive indication of the current state of rate payments, including date of opening the account, date of settlement or last payment, number of payments to date, whether the payer is in arrears, or the account has been written off, together with indicators for charities' allowances and the scale of rate rebates. If a property is associated with bad payments, a program can be directed to one word which is coded to indicate, for each of the preceding five half-years, whether (i) a final demand note

-
- (e) Rating and Valuation Reporter, 1 May 1969, p.290 (No definitive answer could be given)
- (f) Local Government Chronicle, 3 December 1971, p.2242. It is probably not income; if it were, interesting calculations would ensue as to how much more the husband should pay to compensate for the reduced rebate!

was sent, (ii) whether a summons was issued, and (iii) whether a warrant was issued. The one word is therefore a fairly good guide to credit risk.

The files are kept on magnetic tape, and weekly paper print-outs have been kept since the system began work in 1964. If it is necessary to check back through earlier print-outs, then it is possible to follow through by a reference entry in the accounts record, indicating the most recent previous change in the record.

The system prints out the half-yearly rate demands and reminder notices, including the property address and rateable value as required by law. (g)

The compressed coding of the payment record is of particular interest. This was adopted for operational rather than privacy or security reasons, but the entirely non-standard coding makes it almost impossible to guess the meaning of the word without the reference manual. Other data, such as address stored in alphanumeric, would be much more easily interpreted.

Birmingham plans to develop the rating files into the backbone of a property database for the city, and its long-term plans for computer development have been outlined by the City Treasurer. (1)

4. Conclusions

The financial activities of a local authority tend to be more closely regulated by law than others. They are also subject to the scrutiny of the District Auditor, who could reasonably insist on security measures against fraud or intrusion where he felt that public interest required it.

(g) General Rate Act, 1967, s.5

The client is likely to have a mainly pragmatic concern about the implications of details of his financial affairs reaching other agencies or departments. Because financial data lends itself very well to machine handling, exchange of machine-coded data and more ambitious on-line links between agencies would seem to be not too distant. If so, the Treasurer's Department will be drawn into the web of the "cashless society" as much as the local authority database.

The Treasurer's Department in Birmingham also carries a particular responsibility in that it is, in effect, the Computing Department. It was therefore encouraging to find that it has already given some thought to privacy protection, though clearly much further consideration will be needed as the scope of computing facilities is widened.

CHAPTER 10CONCLUSIONS TO PART II

The studies illustrate how difficult it is to generalise about "local authority functions". In some instances, such as education and social work, highly trained staff work with a high degree of autonomy. In other instances, the emphasis is on clerical routine, with awkward decisions being referred upwards through a management hierarchy.

Collectors and users of on-line systems of the future may therefore vary from junior clerks, fresh from school, to social workers with university degrees and years of experience in the field. The maturity of judgment to be expected will vary enormously.

As things stand, very few decisions about privacy are governed by the law. Cases tend to be taken to court only where confidentiality has become an issue in determining another more tangible issue, such as the adoption of a child or the payment of rates on a property. No instance has been found of anyone pursuing a legal claim against an authority purely because privacy had not been respected. Statutory provisions regarding data collection and record-keeping are few in number.

Yet Birmingham's officers on the whole recognise confidentiality as important, and act accordingly. The one sample surveyed indicated that personal obligation to the client outweighed consideration of the legality of disclosure decisions. This implies a strong commitment to the client's interest - where that client is known and identifiable. However, those in clerical posts have to depend on a more general adherence to good practice. It is not really meaningful to talk of a personal obligation to each of

14,000 housing applicants, or 90,000 tenants. Yet even in housing and rating, which were the most bureaucratised of the departments studied, quite a large proportion of the staff meet the public regularly, either in special interviews or over an enquiry desk. They are therefore continually reminded of the human identity of their clients, and in many cases clearly sympathise with their predicaments.

The weaker this commitment to the client's interest is, however, the stronger is the need for formalised privacy protection measures. Most commonly these will take the form of issuing directives to staff, but such measures have a habit of losing ground under stress. For example, policies of ringing back to check on telephone caller's identity are not always implemented when pressure of work is high. Anything which is insisted on as a routine requirement will tend to give way to other routine requirements, so formalisation should anticipate what will happen if load-shedding is necessary.

Two characteristics would seem to mark a good privacy protection scheme.

Firstly, staff should be encouraged to see privacy decisions in terms of the individual they affect, rather than in terms of laws or regulations.

Secondly, if formalised privacy procedures are required, they should be convenient and fail-safe in implementation.

If these characteristics can be built into the computerised environment, a lot of privacy protection should follow as a matter of course.

Suggestions for means to this end are given in chapter 11, post. However,

a major question which remains concerns the means by which such characteristics could be fostered within the computer department itself. At present, computer staff rarely have occasion to meet the public, nor will they usually have had experience in jobs where such contact occurs. They are likely to have followed a scientific or technical career, with political or ethical decision-making playing but a small part.

A programmer or operator may nevertheless aspire to become a systems programmer or a data processing manager. He could then be faced with decisions regarding the management of personal information files, without having any appreciation of the difficult judgments which have gone into formulating the data, or the political tensions which surround its use.

This question is discussed further in 12.3.2.3, post.

PREFACE TO PART III

Modifying the question put at the start of the thesis, how can one prevent the misuse of personal information?

Part III presents some proposals in answer to this question. Chapter 11 outlines a general configuration for systems, which would devolve controls over individ-data and ensure the preservation of context-data. Chapter 12 suggests the legal and administrative measures which would be required to assign responsibilities within such a system. The aim throughout is to support the individ's claim "to influence the decisions, however and whenever taken, whereby information about him is made available to other people" (ante, p.10).

In conclusion, chapter 13 summarises some general findings of the research.

CHAPTER 11

TECHNICAL PROPOSALS

1. Introduction

Earlier chapters of the thesis have identified some of the features of the privacy protection which is likely to be needed in computer-based local government administrations of the future. The requirements are markedly different from those of most situations involving simply data security. This chapter explores the implications of this in designing and implementing systems.

Two main proposals are made:

- (i) that control over some data should be given to the data collector and not to the holder;
- (ii) that circumstances relevant to the privacy of data should be encoded with the data and processed as a "privacy label".

The two proposals are related, but will first be considered separately.

2. Devolved control

2.1. purpose. Computers in large organisations have tended to grow in size, as more and more functions have been handed over to centralised data processing. A single large machine offers considerable attractions compared with several smaller machines of equivalent cost: and increasingly the ability to handle real-time interrogation is seen as one of these attractions. The merits of centralisation have been challenged by some critics, (1) but for the moment, this is the direction in which local authorities seem to be set (albeit hesitantly at times).

A centralised facility will have its access controls determined and implemented at the centre. Yet some of the most effective pressures in favour of privacy protection do not operate at the centre. The collector who identifies with the interests of an indid does not work at the centre. The indid himself is even more remote from the centre. In terms of the information-chain model, controls need to be located early on in the chain: within the system, controls should be available to people at the periphery and not just the centre.

A basic sanction always exists, in that data need not be entered into the system at all. But in an increasingly well-documented society, the absence of information could become as telling as information in more explicit forms. The centralised facility could be particularly well placed for the reaching of negative conclusions of this kind.

Localised control should therefore be provided such that:

- (i) the collector can determine the accessibility of information to other users, (using this as a bargaining point as he chooses);
- (ii) access control patterns can be built up quite independently of the centre's overall control

2.2. implementation. One way of giving someone control over information, without necessarily putting it physically in his possession, is to make him custodian of data necessary for the interpretation of the main data as information. For example, he could be given a cryptographic key, or an index linking names to record numbers. Such data will be referred to as

"indenture-data" (a) by analogy with the method once widely used for linking two parts of an agreement: the agreement (such as one of apprenticeship) would be drawn up as a document which was then cut irregularly down the middle. The patterns of the indented edges provided a link between the two copies. (2)

A suggestion for one way of localising control, using indenture-data, follows. Other techniques might work equally well, and the content and structure of the data is described only by way of illustration.

The central computer installation would maintain three kinds of file.

Firstly, every property would have a unique code (the Ucode), and so would each inhabitant of the property (the Icode). Ucodes and Icodes would be linked to a limited range of basic data items, such as rateable value of property, its use and ownership, and the full name and electoral registration number of each indid.

Secondly, each property would be one of a set based on geographical area, and would be assigned the Acode (aggregate code) for that area. Data referenced by Acode would itself be in aggregate form - for example, a total figure for pensioners living in the area, or a breakdown of the distribution of incomes.

(a) this rather lengthy term has been chosen since other suitable words, such as "key" or "relational data", have tended to acquire other meanings in computing.

Thirdly, central files would be maintained based on the Pcode, to be discussed below.

As well as the central installation, satellite installations would be maintained by the authority's main collector-departments. These installations would have facilities for data entry and printing, and a limited capability for direct-access storage and processing.

The satellite installations would have the facility to assign their own codes (Pcodes) to people or property, and would maintain private indexes linking the Pcodes to the Acodes and U/Icodes. The central installation would provide facilities for data management and storage, organised entirely on the basis of Pcodes.

The central installation would maintain the aggregate files for statistical and planning analysis: the satellite installations would contribute data already sorted into anonymous sets by Acode. The centre would update the Ucode and Icode files on the basis of data passed over by the user departments, as in any conventional centralised system.

The basis of the data organisation can therefore be summarised as:

CENTRALLY

Ucode	Icode	Acode	Data (indid's names, addresses, etc.)	Client flags	Privtype
-------	-------	-------	---------------------------------------	--------------	----------

Acode	Aggregate(i)	Aggregate(ii)
-------	--------------	---------------

Pcode	Data (minimal indid-identifying content)	Privtype
-------	--	----------

LOCALLY

Pcode	Ucode/Icode	Acode	Data (including addresses etc.)
-------	-------------	-------	---------------------------------

Actual data structures and linkages could be much more elaborate than this, providing that the locally stored records retained their function as indenture-data. The "privtype" is discussed in section 3, post. A "client flag" would be set up by any department holding a Pcoded record on that indid, and a copy of the privtype applicable to the Pcode record (ie., in addition to that for the Ucode record itself) might be written to this field. This would enable users to establish whether an indid was known to another department, and something of the nature of the information held about him.

Such a scheme will be seen to have at least two significant drawbacks:

- (i) the processing of data, and particularly the I/O operations would be made slow and awkward in many instances. This would mean frustration for those operating the system, and extra costs for the holder-authority. Some of the penalties, by comparison with a fully integrated database, could be quite high.
- (ii) security would need to be strict at all the satellite installations. If the indenture-data were obtained by an outsider, much of the privacy protection offered by the system would be lost.

The key advantage is, however, that the local authority could retain all the facilities one would expect from an integrated system, without putting individuals' privacy at risk.

For example, the inclusion of the U/I code in each record of the satellite files would make it possible to do very precise matches between different users' files, but only with the active collaboration of both user departments. Analyses could therefore be made using the economy and power

of computer processing, but only under carefully controlled conditions: (for example, the magnetic records might even be handed over to an outside body for processing, with a stipulation that all source records were to be deleted once the output had been created).

Listings by name and address could be produced on the satellite's printer, using the central processor's logic (working with Pcodes), followed by a translation from Pcode to name and address in the local processor. Only sorts based on eg., alphabetic name order would be precluded within the central processor.

Interrogation could be by name or address or even another code, with the indenture-data mechanism being kept quite invisible to the terminal user. Users wishing to access only a few basic files, and maybe exploit the processing power of the computer for calculations or simulations, would be linked to the central processor only.

Finally, since user departments might well want to have localised data entry facilities in any event, these could be conveniently provided for in the satellite installations.

3. Context-data: the privacy label

We now turn to the second of the proposals, which relates to the "context-data" defined in chapter 2, ante. Under conventional filing systems, context-data tends to be preserved by personal contact, or by free-form entries added to documents. Computers tend to reduce the personal contact in administration, by making data readily accessible to users working in widely separated locations; and free-form entries have to be planned for, since the average transaction user will need every

encouragement if he is in any sense to "scribble" into the system.

Before making system-based proposals, the caveat is made that personal contact as a means of preserving context-data is certainly desirable. The following proposals are regarded as ameliorative, certainly not offering any improvement on an office which maintains good working relations among its staff.

3.1. the idea of a "label". There are certain advantages in reducing the context-data to a standard format. These are:

- (i) it means that software can be designed around the format in order to make the entering of context-data quick and convenient: if, on the other hand, collectors had to type in free-form comments, the time needed to do this might deter many people from bothering.
- (ii) the format guarantees efficiency in storing the context-data. While this ought not to be an over-riding consideration, trying to cater for free-form entries capable of being linked to any item of indid-data is likely to demand high overheads.
- (iii) a standard format can avert failures of communication due to ambiguities or idiosyncratic meanings in free-form comments. Equally, it can exclude the use of words or phrases with a high subjective content or emotional overtones: this is not to say that expressions of opinion have no place in public adminsitration, only that they should not go "on the record" as a matter of routine.

It is therefore proposed that context-data should be stored in the form of a privacy label. Such a label would be partly data in its own right, but principally qualifies the indid-data. In the latter sense it has some of the functions of a datatype, so the user of PRIVTYPE as a shorthand name will be adopted.

3.2. the function of PRIVTYPE

Privtype is envisaged as comprising six indicators, as follows:

3.2.1. collector indicator. This indicates who the collector is, and the kind of function in the course of which the data was collected. Part of the coding might be issued to the organisation running the database, as part of a licensing scheme. The rest of the code should indicate which particular person or group within the organisation acted as collector for the data.

Clearly organisations change, and staff move, but an obligation would be created whereby organisations would keep records of the codings allocated among their staff. The exact assignment of codes would have to be a matter for decision in situ: it might be adequate to assign one coding only to the re-housing section of a housing department, for example, while requiring individual codes for housing visitors.

From the coding for the organisation, any subsequent recipient of the data could draw conclusions about the general purpose for which the data was collected. He could also deduce that further dissemination of the data to particular persons or organisations would be undesirable. It may be that in many situations this coding will be redundant: if organisation X purchases a tape of data from organisation Y, it should know about the source of the data. But the passage of time, and the development of large networks,

could obscure even this obvious context-data.

The indicator might be elaborated to give an indication of whether the data was acquired under some special authority, or whether it was acquired for a purpose only incidental to the main work of the organisation.

3.2.2. proscription indicator. The collector indicator automatically defines certain "proscribed" sets, ie., groups of people to whom all access should be denied. For example, a coding for a hospital automatically defines a large number of prohibited users - eg., credit bureaux, assurance companies, social service departments - which it would be cumbersome to catalogue exhaustively. However, certain potential recipients of the data may raise special questions because of their relation to the individ. If we want to prevent certain data from reaching them, it will be easier to proscribe them individually rather than trying to devise complicated rules. An example might be a (adult) daughter who has an abortion and wants to conceal this from her parents, or an employee who is tentatively thinking of moving jobs, but wants to keep any hint of this from his present employer.

3.2.3. reliability indicator. When privacy protection is considered alongside data integrity protection it is sometimes assumed that increased accuracy helps per se in protecting privacy. More often than not, however, the reverse will be true. Many data entries are regarded as private because of their high credibility. I am not concerned if someone surmises that my income is about £30 per week but if someone comes out with the exact figure of £33.80 then I begin to wonder where the information came from.

If data is rated at low reliability, it may cover a variety of circumstances. For example, the collector may have obtained the data from

someone he does not trust, or via a record-keeping system he regards as being badly administered. The circumstances do not need to be distinguished, and in fact there may be positive gains from not doing so. Entering a code that implied that an informant was dishonest might worry some people, whereas they would be willing to enter a general reservation about reliability which did not necessarily cast any aspersions on people standing previously in the information chain.

3.2.4. time indicator. This would give an assessment of the length of time for which the reliability indicator was expected to apply. (In the event of the reliability indicator being of low value, this would of course be of little importance).

Examples here would be assessments of health (an illness, for example, might be stable, suggesting a long-term applicability, or liable to get better or worse), or assessment of eligibility for housing (the client might be in stable circumstances, or prone to domestic upsets and moonlight flits).

3.2.5. retention period recommended. This would enable a collector to indicate the length of time after which the reliability of the data would in all probability be zero, or further retention would present a quite unnecessary threat to privacy.

The coding would represent only the collector's point of view, but this could be given legal significance if any case arose involving data retained for an unwarranted length of time.

The collector might seek to cover himself by always putting a low rating just to be on the safe side. If, however, this also meant that systematic

deletions based on the codings led to him having to replenish the entries, a practical balance might result.

3.2.6. confidentiality indicator. This would be reserved for cases where the data was obtained from the indid under expectations of confidence. A second code might be made available to second holders of data who received data in confidence from the first holder, (ie., data-centred confidence). In either case, the obligation of confidence would extend automatically to all subsequent users, collectors or holders.

As with the preceding code, there may be a temptation to adopt a "safe side" policy, by always entering a high rating. A parallel exists here with the NASA space programme, where it was found that designers were habitually specifying totally contamination-free production environments. Much research and persuasion was needed to arrive at a means of specifying reasonable tolerances for contamination levels. (3) Similarly, policies could be laid down for collectors; but in the last resort, the system could monitor the ratings of each collector and adjust them to make the median equal to a moderate value. It would, however, be essential to make the collector aware of this process if any responsibility were to be assigned to him on the basis of the coding.

3.3. using privtype. In section 2.2, ante, it was indicated that privtypes would be entered on the centrally stored records only. In the U/I code records, the privtype would replace or supplement the client flag, so that if a user wished to establish whether indid X was known to another department, he would not only be given confirmation of this, but the privtype would then be used to generate a message that, say, the indid-data was of low reliability. A user requiring only approximate information

would then contact the collector, who would access the data via his satellite installation in the normal way. A user requiring accurate information would be saved the trouble of pursuing his enquiry. This use of privtypes would however be operable only where the data of the collector in question all had similar privacy connotations.

The main use of privtypes would be in the Pcoded records. Whenever a Pcoded record was accessed, the system would generate appropriate warning messages for printing or display. It would be mandatory for all real-time interrogation programs to include the provision of this display, though with hard-copy output the situation would be more problematic. Here it would probably be preferable to print out a single type of flag to indicate those records carrying exceptionally high privtype ratings. The risk of an extensive listing of privtype ratings falling into the wrong hands would thereby be reduced. A legitimate user of the Pcoded files could still establish the detailed implications of the flag before basing any action on the information, by interrogating on-line. It is to be assumed that any listing of Pcoded records would in any event be accorded high security by the collector-department.

The corresponding risk of someone searching through the computer's records just for those with high privacy ratings is obviated by the storage of the privtype separately from the indid-data (in the case of the U/I code records) or from the indenture-data (in the case of Pcoded records).

3.4. input of privtype. Clearly the creation of privtype codings would need to be an easy matter from the point of view of the collector, and various means could be used to this end, depending on the mode of data entry.

For records being updated regularly, a default privtype could be assigned. This would be linked with each group or item in a schema, (a) depending on the degree of diversity of the indid-data. The central installation would handle the routines necessary for input on-line, which might provide a display of an interpretation of the default privtype, and "menu operation" for the entry of modifications to the default values. Documents for input could have pre-printed indications of the default, and spaces for the recording of any modifications required.

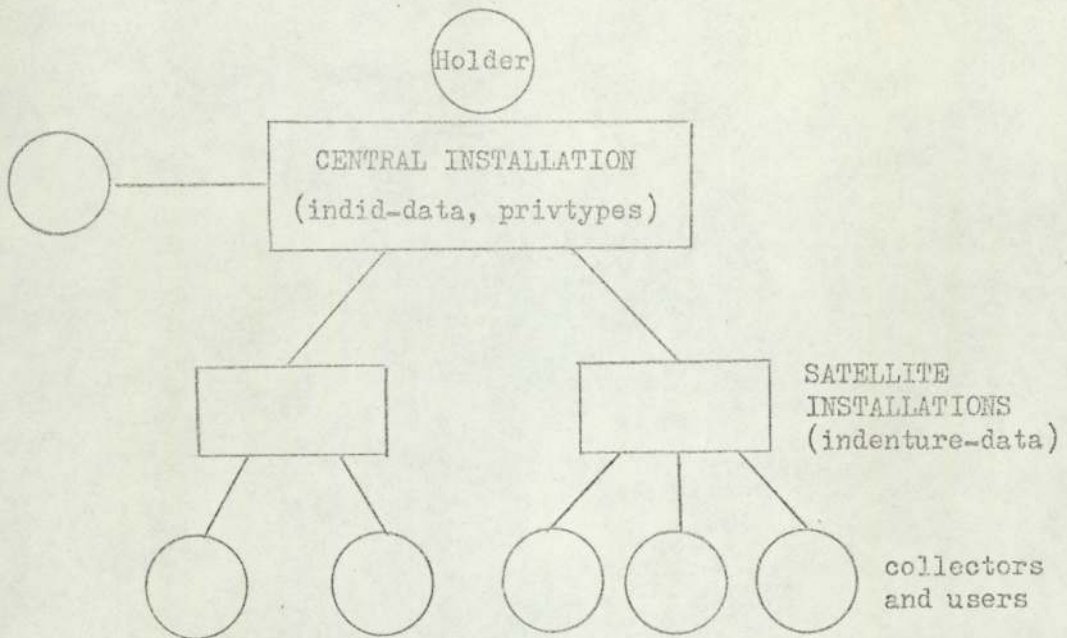
The only entry mode likely to cause problems would be telephone-based or other input where the system could not provide clues to the collector; but it is doubtful whether such techniques would be appropriate for updating personal records in any event.

Examples of the ways in which privtype codes might be entered are given in Appendix 3, and reference (4).

4. The system as a whole

The overall picture of the system can now be summarised as:

(a) in CODASYL DBTG terms



Within the system, certain refinements of control can be envisaged.

Firstly, the collector code for a person inputting data could be deduced by the system from a logging-in code, or from a standard number (such as the personnel number) on the data collection form. Writing operations would proceed only after checks had been made of the collector's authority to input to a particular file, and there would be an update of the collector code in the privtype if necessary. The rules for this would be specified by the satellite installation and implemented by the central installation on the Pcoded data supplied to it. The check on the collector's authority would be independent of any authorisation check made on the person actually controlling data input from the satellite installation.

In controlling read-only access, the central installation could be asked to distinguish between individual users in determining the accessibility of Pcoded records. The pattern of access might be related to the collector codes in the privtype (in cases where more than one collector code was in use under one satellite installation): thus the centre would implement a policy specified by the satellite controller, barring certain users from access to data entered by certain collectors. Other privtype-based or independent constraints might similarly be applied. The constraints could vary: access might be barred completely, perhaps with the system even refusing to acknowledge the existence of the record requested; or the system might interpret and display the privtype only, thus enabling the user to determine the identity of the collector, and to see if the data was appropriate to his needs; or the system might provide a full read-out. All of this would be computed in the central installation, which would have received the request in the form of a Pcode and the enquirer's identity. Since the centre can attach no identity to the Pcode, however, it provides a disinterested technical service: it is only partly conscious of what it is controlling.

The privtype could be used by the central installation for other functions. For example, it could delete data where the period specified in the retention period indicator had elapsed, and generate reminders, based on Pcodes, for data which had not been updated within the period specified in the time indicator. Statistics could be deduced about the cross-flow of information between users of the system, with possible payoffs in improving the data management. The ability to identify the collector and user in each data access might also provide a more accurate basis for assigning costs between users or between user departments.

5. Implementation

With the indenture-data consigned to the satellite stores, the central installation would be free to organise its data in any way it pleased. With certain linkages made impossible, this organisation would be bound to fall short of the rationalisation possible in a complete database. However, the flexibility of storing data on a relational model could be exploited, for example. Also, by virtue of the fact that much of the data would be uninterpretable per se, some of the selective access controls needed in a conventional database would be superfluous.

The privtype would have to be designed in to the system. The two main requirements are that (i) it should be retrievable with its associated indid-data at all times, and (ii) it should be write-protected with regard to everyone except the collector, and even then should be accessible only through special routines designed to produce the appropriate codings. Provision would have to be made for the privtypes to be recorded in the long-term storage devices, but label checks should be such that, when mounted, the device's privtype fields would not be directly accessible to any user. The fields could be placed off bounds to all but the system control program, or a protected buffer mechanism, such as that proposed by Friedman, (5) could ensure that parts of the privtype (particularly the collector code) remained immune to alteration. The protection of privtype fields could be an extension of the general protection of data fields envisaged under Hoffman's formulary system: (6) a modular approach of this kind would make it easier for different collectors to be linked in to the same system routines for privtype decoding, encoding and writing.

While in main storage, the privtype would need to be treated as system information - every bit as immune to user programs as one of the system's

status words. Equally, all functions based on privtype would have to be built into the operating system. Application programmers might be passed privtype values under certain circumstances, but otherwise their interface would be limited to the preparation of parameters to be passed to the encoding routines.

The system as outlined is extendable in a larger-scale or smaller-scale direction. By generating its own indenture-data, or linking local Acodes to larger-scale Acodes, the central installation could transmit data to regional or national databanks for storage. Similarly, it is possible to envisage smaller-scale systems subordinate to the satellite systems, still retaining their own autonomy.

The retrieval of statistical analyses covering the broad scope of local authority activities could not be done with the ease offered by an integrated, on-line planning database feeding on administrative data. However, the Acoded files should yield sufficient information for many planning decisions. More detailed analysis would still be feasible, given the cooperation of the indenture-data holders, and the delays of implementing special procedures to effect such analyses would not be significant in terms of the time-scale of planning. The expense of the procedure might even be less than that of operating adequate access controls on a database offering generalised inquiry facilities (type "D" in figure (i), 4.6, p.100, ante).

In conclusion, the system offers two main advantages. It provides the individ with a more direct influence over the decisions affecting his privacy, through the proxy of the collector. It separates powers, which has always been a pre-occupation of the framers of constitutions (though none of these has yet had so much technological rigidity). The next chapter discusses how these advantages might be applied in local authorities.

CHAPTER 12LEGAL AND ADMINISTRATIVE PROPOSALS

It was suggested in chapter 5 that tensions inherent in local authority administrations will impede the development of coherent privacy policies. Because privacy protection, particularly in the "pragmatic" sense, involves the local authority as a whole, a wider framework is needed, providing sanctions and incentives to promote such policies on a national scale. In some cases, legislation is called for, and in others it would be preferable to rely on administrative practice developed through consultation among authorities and their associated professional groups. This chapter makes proposals for laws and practices which might be adopted. Many of the proposals are related to the technical proposals set out in the previous chapter.

The chapter falls into three main parts.

Firstly, arguments are presented against two proposals which have received support in some commentaries on privacy, but which do not feature in the proposals made here.

Secondly, an outline is given on the way in which databanks in general might be made subject to regulation, in order to provide a context for recommendations relating to local government.

Lastly, proposals are made for remedies which would apply specifically in the local government environment.

1. Strategies proposed to date

1.1. print-out. The right of each individ to be given a copy of his individ-data has been widely supported by academic and business writers (1) and forms an integral part of the U.S.A. Fair Credit Reporting Act, (2) the Swedish Data Act, (3) and Mr. Huckfield's Bill. (4) Notwithstanding this weight of support for print-outs, it is submitted that they have little practical value in protecting privacy. This is not to say that other kinds of injustice may not be discouraged by this means, particularly in connection with credit reporting, but for the moment the effectiveness of print-outs as a protection against intrusive, rather than inaccurate, data collection and storage is considered.

The weaknesses of the remedy are:-

- (i) at best, the individ receives a clear-text version of the individ-data. Because of system innuendo, (a) this may be misleading to the individ. Alternatively, the print-out program may be designed to bias all output in terms flattering to the individ. Both eventualities could be prevented by inspections, but inspections to this level of detail are likely to be sufficient to ensure proper observance of privacy rights on their own.
- (ii) the print-out may indicate what is on the file. But it does not provide any insight into the permitted access paths for users, to and from the file. Details of access could be provided along with the print-out, but to do this comprehensively is likely to add quite substantially to the administrative costs involved.

(a) as defined ante, 3.5.4, p.66

- (iii) checks have to be made that only the indid inspects his own indid-data, otherwise it may be easier for other people to inspect files, by representing themselves as the indids concerned. This could in turn have undesired side-effects, eg., the addition of extra personal information to the file just for this identification process. It again adds to the cost of the print-out procedure. (b) If print-outs are to be mailed out automatically, it has to be remembered that this is not a very secure distribution system, since people may move house, or their correspondence may be quite legitimately intercepted by others.
- (iv) if the indid is to be allowed to appoint a representative to inspect his indid-data, still further checks on the authenticity and proper status of the inquirer will be needed.
- (v) finally, the position would have to be clarified for cases where the indid was under 18 years of age, or mentally ill, or the data referred to two indids jointly.

While it is possible that all these difficulties could be surmounted, few of the procedures for doing so would be suitable for automation. Several conventional administrative procedures would have to be associated with the automated data processing, which could call its net advantage to the operator in question. This is not of course in itself an argument for refraining from introducing such procedures, whether in respect of conventional or computer-based records. However, it places an onus on the advocates of print-out to specify exactly what it would achieve. Since the

(b) For a discussion of costs of print-outs, see Younger Committee Report at para 615

main outcome would seem to be accuracy, and accuracy enhances the effectiveness of surveillance systems, the case for print-outs cannot be taken for granted. Also, if print-outs can only be issued after careful procedures for vetting the inquirer, the nuisance caused by this may in itself deter people from bothering to exercise an inspection right. Given the low rate at which existing rights of inspection are exercised, (c) any print-out provision dependent on inquiry is likely to be ineffective through too little use (even to the point where there is no deterrent effect): and a provision made automatically is likely to reveal more information to more third parties than occurs without print-outs.

1.2. ownership. It is tempting to extend the indid-indid-data relationship into some form of ownership. This was, for example, favoured by the B.C.S. in its evidence to the Younger Committee. (5)

However, the feasibility of conferring such a right is not very high.

Firstly, there is the question of deciding exactly which information "belongs to" the individual. If the ownership were all-embracing, this would stifle all criticism by anyone of anyone else. But once we narrow down the range of information to be subject to the property right, we are likely to encounter confused or only partially accurate versions of the information, and it will be difficult to separate out only that information which is subject to ownership.

(c) the author has on two occasions exercised his right to examine documents held by a local authority. In both cases, it was evident that the staff were not used to receiving this kind of request.

Secondly, if a property right is given to the individual, then other concepts connected with property have to be applied. For example, could the indid assign his property to someone else? Could it be stolen, or converted to improper use, or obtained by deception? Could the indid deny possession to another person? It is this last control which is the one principally sought by the proponents of a property right; but then we have to consider the position of people having a legitimate possession. Since information can be reproduced ad infinitum, large sets of legitimate and illegitimate possessors can be envisaged, with the information passing between them under a variety of circumstances.

Thirdly, possession may be difficult to establish. For example, would "knowing" amount to possession?

Lastly, while there is no difficulty in principle in allowing ownership of property of whose existence the indid might be unaware, there would be problematical analyses to be made where the "property" was created and traded in without the indid's knowledge. If a record is created and then expunged, it is difficult to see the conceptual advantage in giving the indid some kind of retrospective ownership right with regard to it.

Ownership would also have to be less than complete where the indid knew of the existence of information, but good reasons existed for denying him access to some parts of it (for example, in a medical record).

Many of these problems are general to the whole field of the law of intellectual property. However, whereas two companies may be willing to resolve the legal niceties in expensive litigation in connection with information of commercial value, few individuals are likely to be equally keen with regard to the misuse of personal information about them.

2. Proposed method of regulation

2.1. General supervision of all personal-information systems. A national body concerned with good practice in the storage and processing of computerised personal information could fall into one of three broad categories.

- (i) an advisory commission. Like the Medicines Commission or Race Relations Commission, this would have no powers to intervene, but would nevertheless hope to influence and persuade.
- (ii) a regulatory board. This would license or otherwise supervise the operation of computers for certain defined purposes, and so would have a quasi-judicial function. Parallels can be found in the Gaming Board or the Independent Broadcasting Authority.
- (iii) a tribunal. This might also have a licensing function, but would also adjudicate on instances of alleged misuse of personal-information systems.

The Younger Committee recommended system (i), (6), and this recommendation has been taken up by the government. (7) The Control of Personal Information Bill would have instituted a Tribunal - option (iii). The Data Surveillance Bill vested powers in the Registrar of Restrictive Trading Agreements, who would exercise a limited set of type (iii) controls.

The assumption underlying all these proposals is that computer-based systems are sufficiently distinctive to merit special supervision. There is a danger of pursuing this assumption too far, and seeing the issue as computer-centred rather than institution-centred. This seems particularly

to apply when regulation is discussed by computer specialists. Given that demarcation of jurisdiction can cause immense difficulties for litigants (this was, after all, one of the sources of pressure for the reforms of the court system in 1873), any proposal for a new body having adjudicative or regulatory powers ought to follow questions such as: can the jurisdiction be precisely defined? Will it conflict with other jurisdictions?

It is submitted that the rapid development, potential power and technological novelty of computer personal-information systems justify the institution of a body charged with monitoring their progress with an eye to the public interest. This body would also need to be able to inspect installations and their files, and to order changes to be made in file contents or structure, or general working procedures.

The pursuit of individual remedies ought nevertheless to be left to the existing court system. It is true that the courts have shown profound disinterest in computers, and indeed some extraordinary comments have been passed on them. (d) However, if the courts continue to treat computers as a minor innovation, or, even worse, as a technical problem outside their concern, the results will be disastrous in more areas than just privacy protection.

This is not to say that some new remedies should not be provided, and in particular new rules of evidence. But to set up any separate computer-oriented judicial machinery would lead eventually to nonsensical clashes of

(d) eg., "Computers might produce an inaccurate certificate without any negligence on the part of anyone", Ministry of Housing and Local Government v Sharp [1970] 1 All E.R. 1009, at 1024.

jurisdiction and a weakening of the "conventional" court system

2.2. Proposals. A Databank Board would be established. This would be served by an inspectorate and a research department. Appointments to the Board would be part-time in the main, but one condition should be stipulated for any appointee, however eminent: that if his or her experience in either data processing or law were negligible, some coursework or other detailed study in the relevant subject area would be insisted on. The Board ought to be small (say twelve people), and would comprise computer professionals and lawyers in equal numbers.

The inspectorate would be drawn from a rather wider range of backgrounds - including perhaps the police, and other inspectorates. However, the emphasis would again be on recruiting a high proportion of computer professionals, and providing complementary training for everyone. Inspectors would work on an appropriate regional basis: since even national government computer installations are increasingly being sited away from the south-east of England, (e) operations need not be London-based.

The research unit would compile information on developments both in Britain and overseas, and would appraise technical developments in hardware and file systems. Ideally it would develop a consultative role for manufacturers and would-be data holders. It would also provide a forensic service for inspectors, for which it would probably need access to its own secure computer installation.

(e) eg., the installations at Swansea (Department of the Environment), Newcastle and Livingston (DHSS) and Runcorn (Department of Employment).

Government files would come within the jurisdiction of the Board, so it should be evidently independent of any branch of the Civil Service. This has important implications in terms of the way members of the Board should be appointed. Normally, this would be a job for the Lord Chancellor's office, but this office holds extensive personal files, principally with regard to the appointment of people to tribunals and the magistracy.(f) It might therefore become a major user of access to government computerised data, and might even establish its own computer facilities in due course. It is therefore suggested that a majority of positions on the Board should be at the direct nomination of professional bodies such as the Law Society and the British Computer Society, with the remaining appointments being left to the discretion of the Lord Chancellor.

The research unit would be encouraged to operate on a commercial basis where appropriate - for example, by selling publications or charging for consultative work - so that the scope of its work would not be over-dependent on its public funding.

Having thus attempted to make the Board as demonstrably independent as possible, attention must be given to the demarcation which would have to be made of its powers. One of the main criticisms made by the Younger Committee of the Huckfield Tribunal was that its powers were inadequately defined, and in particular a satisfactory definition of the databanks it was to regulate was not provided. The Committee concluded that regulation was

(f) see eg., W. Cavanagh, D. Newton, "Administrative Tribunals: How people become members", 49 Public Administration, pp 197 - 218 at p.203 (1971)

unworkable. (8) It is submitted that in this particular respect the Committee were wrong.

There are three aspects of the problem, which will be considered as follows:- (i) definition (ii) securing evidence of non-compliance and (iii) enforcing compliance.

(i) definition. The Huckfield Bill defines a databank as "any store of information containing details of individuals"; and of the stores so defined only those covering one hundred thousand persons or more would be liable to regulation. (9) No reference is made to filing technology, so conventional records would be included. (10) Some criteria for identifying a "controlled data bank" have been set out by a BCS working party, but some of their definitions for words such as "confidential" and "published" conflict confusingly with normal legal usage, and the scales for sensitivity and accessibility mix together privacy and security requirements. (11)

A definition of a databank subject to regulation is proposed as follows:-

"A databank is any information system in which information descriptive of individual people is regularly stored for periods in excess of one day. It is not necessarily the case that storage or retrieval of the information is organised using personal names, so long as sufficient data is stored to make possible the identification of the relevant information with each individ; (this includes identification made with the aid of other data or other data processing facilities).

"The information-power of a databank shall exceed a critical value if:

(1) the number of indids about whom information is stored exceeds 100,000; or (2) the number of such indids exceeds 10,000, and the stored information comprises a profile of each of them which, by virtue of its extensiveness or private nature, is capable of oppressive misuse against the interests of any indid.

"The information is deemed to be within one information system if information from stores in different places (whether or not these are under common ownership or control) is periodically collated; or, is capable of being collated by any means offering a substantial economic advantage over the collection of not less than one third of the total information in all the stores by requesting it from each indid, there being in law no express prohibition of such collation.

"Any information system having an information-power in excess of the critical value shall be subject to the full jurisdiction of the Databank Board."

(ii) securing evidence of non-compliance. The Younger Committee formed the opinion that, if a regulatory Tribunal could require the production of technical information about a computer system, this would be of use only " ... if information of the kind described would be reasonably likely to enable the Tribunal to know that certain degrees of control were in fact being applied by the "data bank" concerned. The expert advice we have been given is that it would not." (12) From this slender argument the Committee proceeded to their more general conclusion about the unworkability of control.

It is suggested that by specifying three kinds of authority to inspect, it would be possible to secure necessary evidence, without giving the inspectorate unduly intrusive powers. The three kinds of authority are:

(a) Where reasonable grounds existed for supposing that an organisation maintained personal files, an inspector would have a right of entry to any premises where it seemed to him probable that such files might be kept. His inspection would be limited to determining whether the system was of such a type and scale that it might be subject to regulation.

(b) Where an inspector's finding was that, prima facie, a databank of greater than the critical "information-power" existed, or where he felt that his preliminary inspection had been made indecisive by non-cooperation from the data holder, a more formal procedure would be put in motion. The inspectorate would make written requests for details of equipment installed (sufficient for checks to be made with suppliers), and might request copies of documentation and programs. Similar requests, for confirmatory information, might be made to the suppliers of both hardware and software. The inspectorate would not, however, receive actual indid-data in any form. It would be an offence to respond to any such formal request with misleading information, and government departments would enjoy no special privileges compared with any other holder.

(c) Where the inspectorate felt that the evidence available was still indecisive, it could apply to the Databank Board for authority to conduct more extensive investigations. The nature of these would have to be approved by the Board in some detail. In extreme cases, the inspectorate might be authorised to take over the control of an installation in order to run tests on it. The data holder would be entitled to present arguments to the Board, and immunity to investigation could be claimed where it could be shown that the action proposed would jeopardise public safety or national security.

Once the liability to inspection of an installation had been established, the inspectorate could institute procedures (b) and (c) on reasonable suspicion that the configuration of the system, the nature of the data stored, or the working methods used, had changed materially.

- (iii) enforcing compliance. The Huckfield Bill, and the Swedish Data Act, envisage licensing as a means of enforcement. Licensing can have two functions - to restrict the scale of activities, and to lay down the terms for carrying them on. The decision as to the scale of activities felt to be desirable is often political, as for example in deciding how many taxis or street traders should operate in a locality. Once any such figure has been determined, allocation of licenses must be fair (g), and certain obligations in accordance with natural justice arise in changing the figure.
- (h) Nevertheless, the allocation of licences is a less than judicial process, so that, for example, a court may consider evidence normally inadmissible, in deciding whether a licence has been properly withheld. (i)

It has to be recognised that a Databank Board which could deny licences outright would wield considerable power. It could incapacitate organisations which, though objectionable to many people, were not illegal, and a dangerous line of indirect censorship might emerge. For example, might the Board decline to licence the files kept by an unorthodox religious group or by a political organisation? The political implications are wider

-
- (g) eg., Reg v London County Council ex parte Akkersdyk [1892] 1 Q.B. 190
- (h) Reg v Liverpool Corporation, ex parte Liverpool Taxi Fleet Operators' Association, [1972] 2 WLR 1262
- (i) Kavanagh v Chief Constable of Devon and Cornwall [1973] 3 All E.R. 657

than for other activities, such as credit businesses - for which it has been proposed that a Credit Commissioner should assess the "fitness" of people to carry on such business. (j) How do we define "fitness" to operate large personal-data systems? By integrity? Respectability? Orthodoxy?

It is therefore suggested that the Board could only deny a licence altogether on certain specified grounds. These would be limited, and extreme. They might include files tending to supplant those of the police (eg., as might be built up by private security organisations) and files designed to further exploitation of people's weaknesses (eg., a register of sexual deviants). The Board should also be able to resist the establishment of new systems, or extensions to systems, on the grounds that the surveillance capability would concentrate power in the hands of an organisation to an undesirable degree; this criterion would apply equally to public administration, and would no doubt test the Board's political security and independence. But with these exceptions, it would be assumed that every applicant had the right to operate a personal file system. The emphasis in the Board's work should then be on ensuring good practice in the running of the files. Withdrawal of a licence would also be a step not lightly taken, following only on repeated prosecutions for failure to comply with the instructions of the Board.

The main aim of the Board would be to encourage the development of systems which of themselves tended to protect privacy. It should be empowered to insist that hardware be modified, that privacy protection software be improved, or (within bounds) that staff organisation be changed. In these respects, it would be concerned as little as possible

with the content of files, and it should be given wide discretion, such that judicial review of its decisions would be awkward to pursue.

However, the Board might wish to insist on the deletion or alteration of actual data, or of linkages between data. Again, it should only be able to intervene on certain specified grounds. Furthermore, these grounds should be stated in writing, and susceptible to challenge in the High Court. The grounds which are envisaged are:-

- (1) that the data or cross-linkage is not necessary, given the purpose of the holder-organisation: or
- (2) that the data or cross-linkage will have the effect of putting the indid in an unfair negotiating position with regard to the holder. (k)

Economics will tend to enforce provision (1). Provision (2) is designed to cover cases where the data might be related to the holder's business, but is being stored mainly with a view to "leaning on" the indid. The main target would be historical files - say of payment records - which were being retained an unduly long time: in this instance, the time and retention period indicators in privtypes might be material evidence.

The Board would not have the power to order print-outs. Rights to print-outs should be conferred on the indid as and when they are regarded

(k) the strength of the bargaining power of the individual has received legal recognition in the Supply of Goods (Implied Terms) Act, 1973, s.4, and this offers some parallels with the indid/holder relationship.

as necessary (m) The indid would of course be free to bring a grievance to the notice of the inspectorate, with a view to their re-investigating the privacy protection measures of the holder. The inspectorate might also give expert opinion to a court on matters relating to the authenticity of data being introduced as evidence.

Non-compliance with an order of the Board would be an offence. Orders relating to minor aspects of the running of a system could be made by individual inspectors, (n) but any order requiring substantial alteration of procedures or files would have to be issued by the Board, after a full session at which the holder could present his case. Failure to comply with any order could be punished by the Board, after a judicially conducted hearing by them, with moderately severe fines. The inspectorate would act as prosecutor. Serious breaches would be prosecuted by the inspectorate in the Crown Courts, with severe fines and imprisonment of directors as possible punishments. (o) In this way, the problems of arguing relatively minor but technically complicated issues before the Crown Courts would be avoided. Allowing the Board to impose severe penalties would however, be questionable in view of its quasi-judicial composition and function.

(m) see eg., Consumer Credit Bill clause 134

(n) Comparable with notices which safety inspectors will be able to issue under proposed legislation. Department of Employment Consultative Document, June 1973, section 7.

(o) Imprisonment of directors is specifically provided for in eg., Civil Aviation (Licensing) Act, 1960 s.6 (6)

3. Other remedies

3.1. Remedies and offences relating to individual actions. The Younger Committee made two recommendations regarding the rights of the individual: it asked that the law of confidence be reviewed by the Law Commission (para 630), and that a tort of disclosing information illegally obtained should be created (para 632).

The Committee acknowledged that the law was in any case a "clumsy instrument" for seeking privacy remedies, and regarded development of principles through case law as likely to be too slow to keep pace with current conventions (para 42). The re-statement of the law in statutory form would go some way to make litigation more attractive, in that doubts arising from the transfer of principles from the authorities on commercial information would be removed. However, it would not make the law any more responsive to changing attitudes within society, and indeed could have the opposite effect. Much would depend on the exact formulation of the individual's rights: as Dror has pointed out, law can lead or lag with respect to the prevailing norms of society, but will usually be more successful in leading if the matter in question is emotionally neutral. (13) This can hardly be said of confidentiality, with its countervailing forces of curiosity, and the public interest.

The most radical option would be to create a presumption that any personal information divulged by an individual should be deemed to be given in confidence. The recipient of the information would then be barred from passing the information to anyone else at all, without the express consent of the individual. Strictly applied, such a provision would quickly bring

public administration to a halt.

A more practical alternative would be to extend some of the principles of the commercial confidence cases, particularly in giving regard to injury to the feelings of the indid rather than calculable financial loss. It might also be useful to distinguish two kinds of confidence - namely, indid-centred and data-centred. Where information is divulged, the obligation of confidence can be "transmitted" along the information-chain. However, situations can arise, as in the Saunders case (ante, chapter 3, page 51), where X seeks to impose confidentiality on information concerning Y, with a view to keeping Y in the dark both as to the nature of the information and the fact of its being stored. It should be lawful, in respect of such "data-centred" confidence, to pass information to the indid, except where this was being obstructed for the indid's own benefit (eg., a diagnosis of cancer).

The principles of confidence are nevertheless difficult to apply to information chains which run through the various stages of automated data processing, and the creation of two new torts ought to be considered.

Firstly, there could be a tort of obtaining information by deception. Anyone seeking information from an indid and giving a misleading reason for wanting the information would be liable to the indid. The main drawback to such a remedy lies in the unhappy experience of the courts in dealing with other activities involving deception - for example, in the sale of goods (p) and the criminal offence of obtaining goods by deception. (q) There is

(p) eg., in distinguishing innocent and fraudulent misrepresentation, and assessing their materiality to the contract

(q) Theft Act, 1968, s.16

also the point made by social scientists that for certain surveys some deception as to the purpose of the survey is essential in order not to bias the answers the respondent is likely to give.(r) This latter objection could be avoided by making the tort that of deception as to the identity of the collector, or potential holder, of the information. However, a lot of hairsplitting could result in deciding whether the indid was induced to respond by the statement of identity, or by other assurances.

A better solution would be to create special requirements for systematic data collection, whether this was by forms, interviews, or even a computer terminal. Systematic data collection would be defined as the collecting of similar information from an indid-population above a certain size (say 1000 persons) within the period of a year, regardless of the subsequent use of the information. To avoid further problems of definition, it would probably be necessary to include surveys for which anonymity of respondents was envisaged right from the collection stage. It would be an offence not to volunteer details of (1) the name and address of the collector, and (2) the general purpose for which the information was wanted. Particular latitude would be allowed in the latter case in respect of non-commercially oriented research. Many forms and procedures already in existence would in fact meet the requirements. However, any "omnibus" forms for use by different agencies acting together, (s) would need to carry clear indications of all the destinations and purposes envisaged.

(r) See eg., the Younger Committee's own survey (report, p.228); and, "Survey Research and Privacy", Social and Community Planning Research, 1973, at p.22

(s) see ante, chapter 5, p.112

A second possibility in extending the law of tort would be in widening the scope of negligence in handling personal information. Where it might be difficult to trace through an obligation of confidence owed to the indid, he could sue on the basis of a more general obligation to exercise care in the dissemination of personal information. If a failure to do this could be shown to be directly in disregard of specifications from the Databank Board, the indid's case would be strengthened by throwing the onus of proof, against negligence, onto the defendant.

This kind of negligence would not relate to the accuracy of the information, as in the negligent mis-statement cases, but would impose a duty, primarily on holders and users, to check on context-data and the bona fides of people seeking the information. The closest the courts have come to this would seem to be Weld-Blundell v Stephens, (t) where the defendant's negligence resulted in a third party acquiring a libellous letter written by the plaintiff about him. Clearly the moral issues were in conflict, but a substantial minority in both appeals favoured more than nominal damages for Mr. Weld-Blundell, and it was generally accepted that the disclosure was negligent.

The Younger Committee recommended that disclosure should be tortious in different circumstances, viz where the information was such that "... the discloser knows, or in all the circumstances ought to have known, it was obtained by illegal means".(u) Such a measure is unlikely to be very effective unless further legislation is introduced to widen the scope of

(t) [1920] A.C. 956, (H.L.), [1919] 1 K.B. 520 (C.A.)

(u) Younger Committee Report para 632

"illegal means". As things stand, the indid would have no redress where data had been acquired by a variety of forms of snooping. If the illegality amounted to breach of confidence, then the law of confidence itself covers the situation. (v) The main value of the measure might be in providing a civil remedy where a crown employee committed an offence under the Official Secrets Act, (w) or an inspector divulged information contrary to statutory requirements. (x) However, neither of these situations has much relevance to local government.

If the need for such a tort were recognised, it would strengthen the case for making some stiffer prohibitions on the introduction of illegally obtained evidence in court proceedings. Otherwise situations such as that in Ashburton v Pape (y) are going to be further confused.

It would be undesirable to try to widen the tort by basing it on disclosure of information obtained by "improper" or "dishonest" means, since this could make the discloser liable where the acquirer was not - an inequitable result.

(v) see ante, chapter 3, section 1.1.1. ref (k)

(w) Even a person outside Crown employment can of course be prosecuted under the wide terms of s.2 of the 1911 Act. If the Franks Committee recommendations are accepted, there would be value in restricting the tort to personal information, as defined in chapter 12 of the Committee's report.

(x) see ante, 3.3, p.45

(y) see ante, 3.6.4.3, p.78

To summarise, therefore, it is proposed that:

- (1) damages for intangible loss should be readily available in breach of confidence cases, and the individual should have an over-riding interest where confidence is "data centred";
- (2) it should be an offence to undertake certain kinds of data collection without identifying the collector, and stating the purpose of collection;
- (3) a new tort of negligently handling personal information should be created;
- (4) a new tort of disclosing information unlawfully obtained should be created, providing that "unlawful" acquisition were more rigorously defined in other legislation.

3.2. Requirements in local government

3.2.1. The constitution of local government information systems. Certain of the checks and balances to be built into local government information systems will not differ from those for any other information system, and will have to meet the general requirements laid down by the Databank Board.

Other requirements will be peculiar to local government, and it is these with which this section deals. The proposals relate to:

- (a) inspection of records by electoral representatives. At present, a councillor can expect very full reports from the paid officers if a complaint concerning a department is brought to his notice. However, it is extremely unlikely that he will inspect any file himself. The main obstacles to this are practical rather than political, although

in a sense each section in an authority asserts its own privacy with regard to any outsiders. Both the physical difficulties and the antipathy of staff could be overcome by having on-line access to computer files.

For example, a council might resolve that a terminal allowing access to all files held by the authority should be set up, for use by all councillors. There is nothing in law to prevent the council so resolving. However, it is questionable whether even elected representatives are entitled to this degree of surveillance over both their paid officers and the electorate.

A system such as that outlined in chapter 11 would of course create practical obstacles to such wide access, and so councillors might be required as holders, to implement a system which denied them access to all Pcoded files. A further restriction which merits consideration is that a councillor should be able to inspect records only for the electoral unit from which he was elected. Thus a councillor would not be able to access the data relating to indids from other electoral wards of a metropolitan district, or other districts of a county.

In the event of a local government ombudsman being appointed, it would be a source of resentment to councillors if he enjoyed freer access to files than they did. One solution would be to give the ombudsman the right of inspection of all files, but only in person and through the access facilities of the department affected; and perhaps only then on production of a written statement stating the prima facie case against the department. The ombudsman would refer any instances calling for close examination of the system to the Databank inspectorate.

(b) sharing of services. Local authorities have freedom to sell computer services, or share the use of computer systems with other bodies. This freedom needs to be circumscribed. The responsibility for keeping this matter under review would rest with the Databank Board, so that if, for example, the local authority and the local health board wanted to integrate files, the Board might refuse to licence the new configuration. However, it might also be desirable to legislate for a ceiling to the information-power, beyond which no authorities could proceed. This might be defined in terms of more than three or four district functions being supported by an integrated personal-data system for a population in excess of one million people. The LOIA scheme, covering about 900,000 people, closely approaches this limit.

The prospects for integration with national government files make it essential that the national files should be within the terms of reference of the Databank Board. Otherwise one can envisage, for example, the D.E.S. introducing a national system for obtaining its 1 in 10 sample data, with local education authorities using computer files to create the data: and the Databank Board being unable to review the impact of the DES and LEA files taken in conjunction.

(c) "severability". Where local authorities combine together to create joint information systems, a principle of "severability" needs to be introduced. This principle, which would be enacted into law, would make it ultra vires for an authority to commit itself to any joint system from which the authority could not reasonably easily extricate itself in the event of a later change of policy.

The object of this suggestion is to prevent too much power moving away from the participating authorities to a consortium, such that the rights and responsibilities of councillors and ombudsmen outlined above, would become difficult to enforce. There is a broader justification, in that any surrender of power to a consortium makes a nonsense of the separate political identities of the participating authorities - as discussed in 5.4.2 above.

Given the wider political and constitutional issues involved in this instance, enforcement of the provision would not be by the Databank Board, but through the normal mechanism of an order of prohibition, to be sought by any interested party from the High Court. In order to make the mechanism reasonably accessible, the aid of the Databank inspectorate could be enlisted in preparing evidence for the Court, and the inspectorate could be required to furnish evidence to the Court.

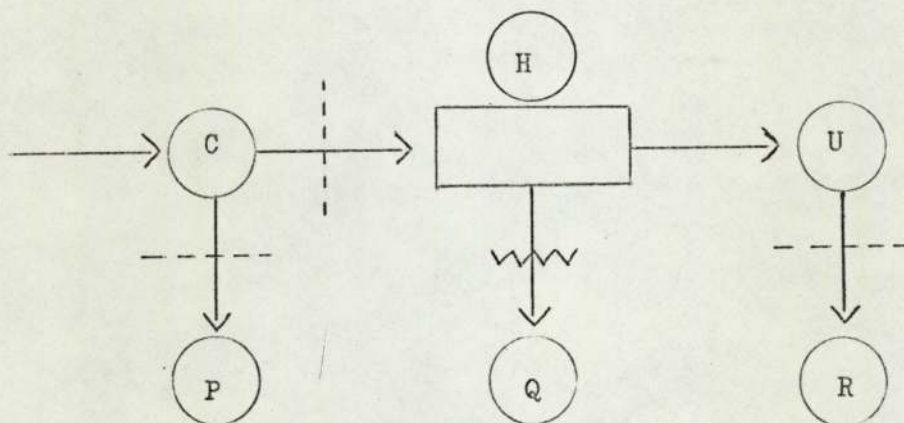
In practice, a constitution would meet the "severability" principle, if it allowed participating authorities to retain substantial indenture-data: to make free use of other computing facilities (there being no question of having to use the consortium system exclusively); to veto access facilities to its own data for all other participating authorities: and to retain copyright in all its files.

3.2.2. Local government officers. The only legal measure to be proposed is that local government officers should be guaranteed the right to refer any cases or practices which worried them to the Databank inspectorate, without fear of reprisal. For example, it might be made explicit in the Code of Good Practice for industrial relations that dismissal on these grounds would be unfair. The right would have to be subject to some provisos, with perhaps a requirement that the matter should first have been

put before a senior member of the authority's staff, and should be based on reasonable suspicion and not malice.

Otherwise, responsibility would be fixed mainly on the authority as holder, to implement a system incorporating features of devolved access control and privacy labelling, in accordance with directives of the Databank Board. An authority taking its responsibilities in the fullest sense would encourage appreciation among its staff of associated factors, such as the importance of using only "appropriate" information in decision-making. (z)

The division of responsibility between officers, and between officers and the corporate body, can be more exactly defined. Let us consider this in terms of a typical set of circumstances:-



For example, information might be obtained by a Housing Visitor, (C) and retrieved by a clerical officer in the Transfers Section (U). Privacy infringements might result if:

- (1) the collector acquires the data by unlawful means or from someone else who has used unlawful means. It would then be tortious (under the

(z) this concept of "appropriateness" is being developed as part of the research study at the Norwegian Research Center for Computers and Law. see page 9, ante

proposals made earlier) to give the information to anyone, including the authority as holder. If the collector disregards a confidentiality obligation to the indid, or treats the data negligently, then the data could find its way improperly to P. Confidence lies between the collector and indid, and the holder could not be liable for any breach. Data-centred confidentiality might have been created by the collector's contract of employment, in which case he will also be liable to the holder as employer. The holder could be vicariously liable for disclosure of data obtained by illegal means, even, theoretically, if the disclosure was to the holder himself; and the holder could also be vicariously liable for negligent handling of the information, except where this could be attributed directly to the holder in not instituting proper administrative procedures

- (2) the holder puts inadequate technical controls in his database. Consequently, data is retrieved by Q. This might of course result from a breach of directions from the Databank Board, in which case an offence would have been committed by the breach alone. However, as with safety legislation, the indid ought to be able to base a civil claim on the breach. Also in line with safety laws, it might be desirable to create some strict liability of the holder in these circumstances, so that the holder would be liable even if the faults originated with outsiders, such as a manufacturer or software house. (a)

(a) cf Employer's Liability (Defective Equipment) Act, 1969, s.1.

What, though, if Q actively broke through the technical controls? There is little legal authority to go on. Part of a normal duty of care can include taking reasonable precautions against burglary. (b) but determining what are reasonable levels of protection against crime can be a rather sticky question. (c)

- (3) the user passes data on to R. If this could be shown to follow from a failure to note and act on PRIVTYPE warnings, liability would rest with the user for negligent information handling. A failure to provide proper privtype warnings might be a system failure (ie., a holder responsibility), or a failure to input them in the first place (ie., a collector responsibility). The holder would be vicariously liable for either the user's or the collector's actions, so long as they occurred in the normal course of their duties.

Questions might arise as to the reasonable level of skill which a collector or user would be expected to show in handling information. For example, the expectation might be higher for a social worker or teacher than for a clerical officer in a housing or rates department. In practice, rulings of the Databank Board would ensure that difficult decisions would not normally be left to junior or inexperienced employees. Where, however, negligent handling of information resulted from decisions having to be taken by someone who could not reasonably be expected to cope with them, a

(b) Stansbie v Troman [1948] 2 KB (decorator went out to get wallpaper and left front door unlocked)

(c) see eg., Lord Pearson in British Road Services Ltd v A.V. Crutchley [1968] 1 All E.R. 811, at 818, 820.

presumption would be created that the authority as holder was negligent, in not establishing proper procedures. To avoid liability, the authority would then have to prove that the situation giving rise to the misjudgment was so unusual that it could not reasonably have been foreseen, and allowed for in their administrative procedures. Where the user was someone skilled in computing and allowed privileged access, very high standards might reasonably be expected.

3.2.3. professional responsibility. At present, it seems very improbable that a dominant professional group will emerge in local government computing. The staff of computer sections tend to reflect their background in Treasurer's Departments, and hold accountancy qualifications (particularly those of the IMTA). Newer staff may be more computer-oriented, and if local government computing is seen as one step in a computing career, then membership of the British Computer Society may be more attractive to them. As time goes on, local government computing is likely to absorb people from other professional groups, as it widens the scope of its activities.

The prospects for regulation by a professional body, giving rulings on conduct, similar to those of the legal or medical governing councils, are therefore small. But professional attitudes might be encouraged in other ways. The information and education services of LAMSAC might be extended further in this direction: the Committee has already published guidance for local authorities on privacy, though there is little contained in it that is specific to local government. (14) The Committee would be a natural focus for discussion of other social implications of local government computing.

The problem mentioned in chapter 10, of technically trained personnel moving into jobs where they are faced with decisions concerning personal

information, merits more direct attention. Authorities might lay down requirements for their computer staff which would ensure that they had some appreciation of the circumstances surrounding the collection of personal data. This might take the form of assigning a programmer to a team of housing visitors for one day a week, or seconding the computer room shift leader to a social services office for a month. The nature of privacy-risk situations, and the dilemmas facing data collectors, might be brought home in a way which is unlikely to follow from the study of abstract codes of conduct.

3.2.4. Outside contractors. The local authority may wish to put its database operation in the hands of a bureau, or engage "security consultants" to implement technical controls in a system run by their own staff.

The bureau or consultant would in these circumstances be under a contract for services, and so the authority would normally avoid vicarious liability for any acts of the contractor or his employees.

However, it might be desirable to stipulate that for the purpose of determining tortious liability, any such arrangement would be deemed to be a contract of service. Otherwise, the indid might be faced with an overwhelmingly difficult task in fixing liability on one party or the other.

CHAPTER 13CONCLUSIONS

The thesis began with an operational definition of privacy, namely, the claim of an indid to influence decisions whereby information about him is made available to other people. It seems that these decisions can be taken in three ways.

Firstly, there is the collector who knows the indid personally, or else knows a good deal about the indid's circumstances, who can base his decisions on this direct personal knowledge.

Secondly, there is the user, or other recipient of the information via the information system, who knows less about the circumstances surrounding the acquisition of the data but who can usually find out about these if he wants to.

Lastly, there is the creator or holder of a databank, who builds automatic controls into the information system which the databank serves. These must be based on general prescriptions and so cannot really take account of individual circumstances.

The computer fraternity is mainly interested in these automatic controls, which have received a disproportionate amount of attention to date. Some such controls will be needed in any system, but plenty of techniques are available, and research in this area is liberally funded.

The lawyers, on the other hand, prefer to consider situations of the first kind. As Professor Cowan has pointed out, lawyers like to

individuate: their skill is in dealing with human interactions. I would press the point further, and suggest that lawyers tend to see computers as being quasi-human; or at least they are reluctant to abandon their human-value-thinking in discussing computers. The result is that insufficient attention is given to questions such as the impact of computers in assigning responsibilities within institutions, or the dependability and accessibility of evidence. Instead, "the computer" tends to be cast in a role, which none of the huge variety of configurations, present or proposed, can really fit: one might just as well look for the truly typical "transport device" or "building".

This leaves unexamined the in-between area of privacy protection, where data has passed into the system, and is available for use in decision-making by someone remote from the source. I believe that a prescriptive, automatic system can filter out data having privacy-risk implications with only limited efficiency. One cannot argue simply "this data D must never reach user X". For one thing, we are unlikely ever to agree on the basis for prescribing X's access to D. For another, the data will have as many implications as there are users and circumstances. The computer view needs to be modified by some of the ideas applied in law - particularly in thinking of privacy-risk situations or occasions, rather than private data.

The people closest to the problem already, in the context of local government, are the middle management, and the clerical staff. Unfortunately, the computer community, anxious to see the impact of computer databanks in toto, tends to seek information from senior management. Academic surveys, such as those of A.F. Westin or the Canadian government's task force, have also depended on the assessment of people who direct, rather than carry out, the routine operations.

Meanwhile, the lawyers have shown concern over the political significance of databanks, and the wide issue of individual privacy, but there is an astonishing shortage of research into how the law actually works. A heavy weight of respectability rests with abstract and theoretical studies, which badly needs to be balanced by appraisal of what laws do, or fail to do, particularly in the grey areas of quasi-judicial decision-making. Unless more investigation is forthcoming, the legal profession risks finding itself in much the same position as those medical men who clung to Galen in the age of Harvey.

Certain specific investigations are, I believe, required.

Firstly, more observation should be made of the way confidentiality is actually handled in the day-to-day business of local authorities, and more attention should be paid to the attitudes and views of the people who work at this level. It is no reflection on senior officers to say that most of them have no more than a general idea of the way judgments on privacy are actually being made. There is no way they can make an accurate assessment, since the arrival of a manager in any office ensures that everything proceeds by the book from that moment on, and any breaches of confidence that there are will rarely have clear-cut repercussions of a kind resulting in a report going up the line. However, the independent observer, using due patience and discretion, can expect to find rules being bent in a number of ways. It is my impression that much of this rule-bending is helpful, healthy and more often than not to the benefit of the indid. Reporting such observations raises obvious difficulties, and arriving at definite conclusions is equally difficult; also, as Rule discovered, any suggestion that the rules are not being strictly adhered to will upset the senior management. (2) However, the delicate area of official versus unofficial

norms in respect of privacy merits further investigation. To introduce systems based entirely on the official norms may invite some curious developments in the unofficial ones.

Secondly, more technical research should be devoted to means of giving collectors and users of data control over the data they handle, without sacrificing too many of the advantages of the database approach. The system must also be able to provide explicit mechanisms for some of the informal or unofficial means which these people currently use in protecting privacy - adding comments, "losing" information, and so on. Over-powerful control by any one individual should also be denied. A number of possibilities exist for meeting these criteria, but all need practical evaluation.

Thirdly, aspects of the previous two suggestions could be combined, in trying to develop more sophisticated models of the way personal information is actually interpreted and used in systems.

Fourthly, there are three application areas outside local government where study might be focussed. One is the use of on-line facilities for retailing, and other points of contact with the public. Then there are the schemes now emerging for computer/cable television networks. Finally, there is the introduction of surveillance systems in law enforcement. Each of these developments raises questions of a special kind. It is difficult to see any of them becoming realities, threatening or otherwise, much before 1980. Nevertheless, a lot of the characteristics of the problems they could raise are capable of investigation now.

Apart from research, certain practical steps can be taken quite quickly. Those which would require legal reform have been outlined in the previous chapter. However, local authorities and computer manufacturers might consider the following proposals:

- (1) it is possible that a manufacturer may have reservations about supplying a particular facility to an authority - for example, the councillors' access facility discussed in chapter 12. It might be advisable to anticipate any such conflict of opinion by inserting a clause in the contract of lease or sale. This would enable the manufacturer to insist that any aspect of the configuration which raised serious questions concerning privacy, or any other social impact of the system, should be referred to a meeting of the full council, in the form of a motion designed to clarify the issue. The manufacturer would not necessarily contribute to the discussion, but would be accepting a responsibility to draw attention to the possible undesirable consequences of a system's implementation, which councillors and officers not versed in the technicalities of computing might otherwise not see. The industry cannot reasonably claim to be taking an ethical stance on such issues unless it is prepared, where necessary, to grasp the nettle in this way.

- (2) where a local authority and manufacturer are jointly developing an on-line personal information system, they should consider the appointment of a "privacy analyst" to the development team. This need not be a full-time responsibility, but if part-time, should be assigned to someone not otherwise engaged in the project. The person appointed would be kept informed of all developments proposed, and would assess them purely in terms of privacy-risk situations. He would be obliged to report his conclusions regularly to the team.

It is suggested that someone whose profession regularly involved decisions about confidentiality, such as a social worker or psychiatrist, might be seconded to this task.

- (3) Finally, local authorities could pave the way for sound privacy protection in the computerised environment by providing all their staff who could be regarded as potential computer users with an appreciation of what computer systems are and what they can do. This might help to de-fuse some of the antagonism which undoubtedly exists towards computers, particularly among clerical workers who see themselves as being automated out of their jobs.

With a staff already familiar with the concepts of on-line working, the authority could give attention to evolving its system of privacy protection, rather than fighting a rearguard action over the very introduction of the computer.

From this point of view, as from others, privacy needs to be appraised now. It is a weak flower, and will not survive long on any kind of battlefield.

REFERENCESINTRODUCTION

(pages 6 - 13)

1. J.B. Rule, "Private Lives and Public Surveillance", Allen Lane, 1973, at p.23
2. S.I. Benn, in "Privacy", ed. J.R. Pennock and J.W. Chapman, Atherton Press N.Y. 1971, chapter 1
3. Ibid at p.12
4. R.D. Blekeli et al, "Information Handling and Privacy. A case study of the Directorate for Seamen". (Preliminary title) Oslo, 1974, forthcoming. K.S. Selmer, "Standards for Information Handling and Control Procedures", Oslo, 1974.
5. E.L. Beardsley, in ref.(2) supra at chapter 3
6. R.P. Lowry, "Toward a Sociology of Secrecy and Security Systems", Social Problems, Vol.19 pp 437 - 450, 1972

CHAPTER 1

(pages 14 - 22)

1. E.A. Shils, "The Torment of Secrecy", Heinemann, 1956.
2. Findings of the Conference of Privy Councillors on Security. Cmd 9715 (1956)
3. Committee of Privy Councillors on Interception of Communications. Cmd 283 (1957)
4. "Security Procedures in the Public Service", Cmd 1681, 1962
5. The Bill, along with two later Bills, is reproduced in Appendix F of the report of the Younger Committee
6. B. Neill, "The Protection of Privacy", 25 MLR 393 - 405, at p.401
7. C. Kaysen, Report of Task Force on Storage of and Access to Government Statistics, Bureau of the Budget, 1966
8. Hearings on the Computer and Invasion of Privacy: before a Subcommittee of the House Committee on Government Operations, 89th Congress, 2nd session, July 1966. The Hearings were published as a hardback book by the Arno Press, New York, in 1967, under the title: "The Computer and Invasion of Privacy".

9. In "Privacy and Efficient Government: Proposals for a National Data Center" 82 Harvard Law Review p.400 (Dec. 1968); and A.R. Miller, "The Assault on Privacy", University of Michigan Press 1971, pp 54 - 67.
10. C. Kaysen, "Data banks and dossiers", 7 The Public Interest pp 52 - 60 (Spring 1967): "I conclude that the risky potentials which might be inherent in a data center are sufficiently unlikely to materialise so that they are outweighed on balance, by the real improvement in understanding of our economic and social processes this enterprise would make possible". (at p.60)
11. E.G. A.R. Miller, "The National Data Center and Personal Privacy", Atlantic Monthly. Nov. 1967 p.53; Denault et al, "Project: The Computerisation of Government Files: What Impact on the Individual?" 15 U.C.L.A. Law Review 1380 (1968); J. Sawyer and H. Schechter, "Computers, Privacy and the National Data Center", 23 American Psychologist 810 (1968)
12. M.V. Wilkes, "A World Dominated by Computers?", in "The World in 1984" Vol. 1, ed. N. Calder, Penguin, 1965.
13. L. Bagrit, "The Age of Automation", Pelican, 1966
14. N. Calder, "Technopolis", MacGibbon & Kee, 1969, p.217
15. See eg., A. Mitchell, "Big Brother 1969", Sunday Times, 2 March 1969; Clive Jenkins, of ASTMS, also captured the headlines with the subject when he inaugurated Datafair 69.
16. Society of Conservative Lawyers, "Computers and Freedom", Conservative Research Department, 1968
17. Right of Privacy Bill (Alexander Lyon, M.P.) 1967, and Right of Privacy Bill (Brian Walden, M.P.) 1969. During the second reading of the latter Bill, Mr. Callaghan, then Home Secretary, announced that a committee would study the privacy issue under Kenneth Younger: Hansard, Vol. 794 Col 941, 23rd January 1970
18. D. Madgwick, "Privacy under attack", NCCL, 1968
19. Justice, "Privacy and the Law", Stevens and Sons Ltd, 1970
20. A.F. Westin, "Privacy and Freedom" 1967 (British edition by Bodley Head, 1970); "Information Technology in a Democracy" (ed.) Harvard University Press, 1971; "Databanks in a Free Society" Quadrangle Books, 1972
21. Four articles are listed in the bibliography, post
22. U. Thomas, "Computerised Data Banks in Public Administration", 1971 and G.B.F. Niblett, "Digital Information and the Privacy Problem", both in the OECD Informatics Series

23. "The protection of privacy", complete edition of UNESCO international social science journal, Vol. 24, No. 3, 1972; a report on computer databanks in government has been commissioned by UNESCO from Dr. W. Dohr of Vienna University; an international survey by A.F. Westin is due to be published in 1974
24. J. Jacob, "Computers and Privacy", New Law Journal, 3rd July 1969, p.633; "Seven dangers of computers", New Society, 11th December 1969, p.940; "Confidential Communications" and "Protection of Privacy" (jointly with R. Jacob), New Law Journal, 6th/13th February 1969, pp 133 and 157; "Data Banks, the Computer, Privacy and the Law" issued by NCCL, 1969; "A New Attempt to Control Data Banks", Law Guardian April 1971, p.19
25. G.B.F. Niblett: "Computers and Privacy", BCS Computer Bulletin, December 1969, p.431; see also reference 22 above
26. C. Tapper, "Computers and the Law", Weidenfeld and Nicolson, 1973, particularly chapter 3
27. B.C.S. Code of Good Practice, 1972, section 5.2; BCS Privacy and Public Welfare Committee, "Privacy and the Computer - Steps to Practicality" 1972
28. The proceedings have since been published by the National Computing Centre Ltd under the title "Privacy, Computers and You" (1972)
29. See eg., Smythe, "The Databank Society", Computer Weekly, 12th November 1970 p.1; Hawker, "Why we need a Thought Police", New Scientist, 12th November 1970 p.336, among the media "warm-up" for the conference; reports and editorials followed in the "Times" and "Guardian", 19th - 20th November 1970
30. CSD reports appeared in January and February of 1971, but neither makes any significant reference to privacy. The first was in any event commissioned from outside consultants and published belatedly. CSD, "Computers in central Government Ten Years Ahead", HMSO; and Minutes of Evidence to Sub-Committee A of Select Committee on Science and Technology, 17th February 1971, HMSO (267-iii)
31. Hansard Vol. 810, Col. 1465, (2nd February 1971). The Bill was lost at second reading - Hansard Vol. 816, Col. 1913 (7th May 1971). An identical Bill was introduced by Mr. Huckfield in 1972 - introduced on 8th February, and lost on 2nd reading on 21st April,
32. Eg., "Is 1984 here?", The Economist, 6th March 1971, p.54; US forces pry into 25 m private lives" Sunday Times, 7th March 1971; "Data bank fears", New Scientist, 1st April 1971.

33. Eg., N. Foy, "A bonfire of census forms", *New Scientist*, 15th April 1971, p.132; editorial, "A Question of trust", *The Guardian*, 17th April 1971; "The Census - Doing the Privacy Thing", *New Law Journal*, 22nd April 1971, p.331. Opposition stemmed mainly from the NCCL, the Liberal Party, and a "Census Concern Committee", centred on Chelmsford, Essex.
34. The author is indebted to G.P.F. Boston, head of the Census processing operation, who discussed this at some length: Titchfield OPCS Office, 15th October 1971
35. White Paper, "Security of the Census of Population", HMSO, Cmnd 5365, July 1973.
36. Eg., written answer by Sir Keith Joseph, *Hansard*, Vol. 816, Col. 309, 4th May 1971; oral answer by Patrick Jenkin, *Hansard*, vol. 817, col. 1054, 18th May 1971; and written answer by Joseph, vol. 823, col. 287, October 1971
37. Minutes of Evidence to Sub-committee A of Select Committee on Science and Technology, 6th May 1971, HMSO (267-xi); the previous BCS evidence was to the Committee's predecessor (Sub-Committee D) on 11th March 1970 and contained no mention of privacy
38. "Guardian", 11th May 1971
39. Oral reply by Prime Minister, *Hansard*, vol. 818, col. 230, 25th May 1971
40. Some of the results are to be included in a White Paper late in 1973; statement by Mr. Robert Carr, *Hansard*, vol. 859, col. 1968, 13th July 1973
41. Written question to Mrs. Margaret Thatcher, *Hansard*, vol. 820, col. 425, 8th July 1971.
42. *Hansard*, vol. 822, col. 487, 27th July 1971
43. Report of the Committee of Privacy, July 1972, HMSO, Cmnd 5012; Departmental Committee on Section 2 of the Official Secrets Act, 1911, September 1972, HMSO, Cmnd 5104
44. *Hansard*, (House of Lords) vol. 343, col. 104, 6th June 1973; *Hansard*, vol. 859, col. 1955, 13th July 1973.
45. "Privacy, the Press and Mrs. X", *New Law Journal*, 20th July 1972 pp 666 - 667
46. C.C. Bennett, "What Price Privacy?", *American Psychologist*, May 1967, pp 371 - 376
47. Review of "Privacy and Freedom" by A.F. Westin: F.H. Newark, 87 LQR, 264, April 1971

CHAPTER 2

(pages 23 - 41)

1. LOLA stands for "London On-line Local Authorities". The four authorities concerned are: Hackney, Haringey, Hillingdon and Tower Hamlets.
2. M.D. Mesarovic, D. Macko, Y. Takahara, "Theory of Hierarchical, Multilevel Systems", Academic Press, 1970
3. The test of what a "reasonable man" would have done or decided in the situation is usually applied in connection with negligence. The reasonable man is not expected to be absolutely reasonable, but rather an embodiment of what is normal and sensible. Needless to say, the application of this kind of test has given rise to numerous controversial cases.
4. B. Sundgren, "Security & Privacy ..." bibliography 165.
5. See eg., the attitude survey commissioned by the Younger Committee (Appendix E of their report), also R.E. Anderson, "Sociological analysis of public attitudes towards computers and information files", Spring Joint Computer Conference 1972, p.649
6. Legislation covering credit bureaux has been promised: written answer by Sir Geoffrey Howe, Hansard, vol. 856, col. 221, 11th May 1973
7. Note that liability, which derives from Hedley Byrne v Heller [1963] 2 All E.R. 575, has not been extended to give the indid any right to sue. In fact, cases tend to be of the kind where the indid has benefitted and the user has suffered loss, because money or some other benefit was given to the indid on the strength of the indid-datum
8. C. Fried, "Privacy", 77 Yale Law Journal 475 (1968)
9. M. McLuhan, "Understanding Media", 1964, McGraw-Hill, Chapter 2.
10. "Identifier" and "descriptor" are the terms used by the study team who devised the "General Information System for Planning", HMSO, 1972. Terminology varies a great deal: CODASYL's and other more theoretical discussions tend to talk of NAMES and VALUES.

CHAPTER 3

(pages 42 - 82)

1. Report of the Committee on Privacy, Cmnd 5012, Appendix I, p.287
2. Justice, "Privacy and the Law", Stevens, 1970
3. L.E. Mallett, "Privacy", in Meek et al, "Computers and the Year 2000", NCC Ltd, 1972, chapter 20

CHAPTER 3 (continued)

(pages 42 - 82)

4. C. Tapper, "Computers and the Law", Weidenfeld and Nicolson, 1973, chapter 3
5. 13 M.L.R. 281 - 306 (1950); 21 M.L.R. 661 - 668 (1958);
26 M.L.R. 412 - 417 (1963)
6. For a summary, see Younger (ref. 1 above) pp 314 - 318; also, L. Brittan, "The Right of Privacy in England and the United States", 37 Tulane Law Review 2235, (1962); H. Kalven, "Privacy in Tort Law: were Warren and Brandeis Wrong?" 31 Law and Contemporary Problems, 326 (1966)
7. See eg., E.V. Comber, "Management of Confidential Information", 1969 Fall Joint Computer Conference, AFIPS, p.135 at 137
8. Law Reform Committee, 16th report. Cmnd 3472, HMSO, 1967, at p.3
9. G.D. Nokes, "Professional Privilege", 66 L.Q.R. 88, 1950
10. C. Tapper, note on Butler v Board of Trade (1970), in 35 M.L.R. 83 - 87 (1972)

CHAPTER 4

(pages 83 - 103)

1. W.H. Ware, "Security and privacy: similarities and differences". ACM Spring Joint Computer Conference (hereafter "JCC"), 1967, pp 287-290
2. IBM Manual, "OS/MVT with Resource Security" GH20-0967-0
3. Ibid, p.23
4. M.A.L. Farr, B. Chadwick, K.K. Wong, "Security for Computer Systems", NCC Lrd, 1972
5. A modem at this price was exhibited by Modular Technology of London, at Datafair 73
6. J.D. Babcock, "A brief description of privacy measures in the RUSH time-sharing system". ACM Sping JCC, 1967, at p.301
7. IBM Manual GA 27-3039-0
8. News item, "Device Guards Data Files", Computer Weekly, 2nd August 1973 at p.9. Device marketed by Trium Co. Ltd.

9. See eg., I. Berenyi, H. Bushby, "Identification at their fingertips", Computer Weekly International, 9th March 1972 at p.7; W.S. Mohn, "Two Statistical Feature Evaluation Techniques Applied to Speaker Identification" IEEE Transactions on Computers, vol. C-20, No. 9, pp 979 - 987; C.N. Liu, G.L. Shelton, "Computer-assisted fingerprint encoding and classification", IEEE Transactions on Man-Machine Systems No. 3, pp 156 - 160
10. D.R. Cone, "Personnel Identification by Hand Geometry Parameters", S.R.I. Report of July 1969
11. IBM Manuals G510-0739, SC34-1532-0
12. IBM Manual GH20-0967-0 at p.6
13. IBM Manual GH20-0892-0 at p.11
14. IBM Manual GH20-0911- at p.4.3
15. IBM Manual 320-1014-1 at p.3
16. See eg., M.G. Stone, "A matter of privacy", Data Management, December/January 1971 at p.14
17. R.F. Farag, Y.T. Chien, "Online signature verification", ONLINE 72 Conference proceedings, pp 403-424
18. No public reports on this research are available. However, the free-hand input terminal developed for the experiments is now marketed, together with character-recognition programs, by Quest Automation of Wimborne
19. R.W. Conway, W.L. Maxwell, H.L. Morgan, "On the Implementation of Security Measures in Information Systems", 15 Comm. A.C.M., No. 4, April 1972 pp 211 - 220
20. Ibid, at p.216
21. T.D. Friedman, "The authorisation problem in shared files", IBM Systems Journal, No. 4, 1970, pp 258 - 280
22. Ibid, at p.267
23. C. Weissman, "Security Controls in the ADEPT-50 time sharing system", ACM Fall JCC, 1969, p.119
24. R. Conway, W. Maxwell, H. Morgan, "Selective Security capabilities in ASAP-A file management system", ACM Spring JCC, 1972, p.1181
25. L.J. Hoffman, "The formulary model for access control and privacy in computer systems", SLAC-117 (Atomic Energy Commission) 1970 at p.12

CHAPTER 4 (continued)

(pages 83 - 103)

26. L.J. Hoffman, W.F. Miller, "Getting a Personal Dossier from a Statistical Data Bank", Datamation, May 1970, pp 74 - 75
27. B.W. Lampson, "Dynamic Protection Structures", ACM Fall JCC 1969 pp 27 - 38
28. Reference (4) above at 5.3.1.10
29. C. Weissman, "Trade-off Considerations in Security Systems Design", Data Management (USA), April 1972, vol. 10, pp 14 - 19 at p.19
30. E.L. Glaser, "A brief description of privacy measures in the multics operating system", ACM Spring JCC 1967, p.303
31. Codasyl Systems Committee, "Feature Analysis of Generalised Database Management Systems", 1971
32. D.K. Hsiao, "A File System for a problem-solving Facility", PhD thesis, University of Pennsylvania, 1968 at p.52
33. R.M. Graham, "Protection in an Information Processing Utility", 11 Comm. ACM, May 1968, pp 365 - 369
34. B. Sundgren, "Security and Privacy in Statistical Databases", Swedish Bureau of Statistics, 1972; I.P. Fellegi, "On the Question of Statistical Confidentiality", Journal of the American Statistical Association, March 1972, pp 7 - 18; R.F. Boruch, "Relations among Statistical Methods for Assuring Confidentiality of Social Research Data", Social Science Research 1 (1972), pp 404 - 414; M.H. Hansen, "Insuring Confidentiality of individual records in data storage and retrieval for statistical purposes", ACM Fall JCC 1971, pp 579 - 585

CHAPTER 5

(pages 104 - 117)

1. Maud Committee, "Management of Local Government", HMSO, 1967, at paras 68, 194
2. Royal Commission on Local Government in England, Cmnd 4040, 1969, at para 110
3. Reform of Local Government in England, Cmnd 4276, 1970, at para 18
4. Local Government in England, Government Proposals for Reorganisation, Cmnd 4584, 1971, at para 14
5. The New Local Authorities, management and structure. Report of Study Group, HMSO, 1972

6. Wellbeloved and Burke, "Ombudsmanic depression", Local Government Chronicle (hereafter LCC), 18 November 1967, p.1917; N. Johnson, "An ombudsman for local government?", LCC, 6 July 1968, p.1043; K.P. Poole, "Organising the Ombudsman", LCC, 1 November 1969, p.2074. A vague government commitment appears in ref (4) at para 52, and a consultative document on the subject was issued by the Department of the Environment in May 1972
7. Memorandum in response to Department of Environment consultative document, County Councils Association (duplicated, undated)
8. Ref (5) above at para 3.20
9. Eg., Public Health Act, 1936, s.248 (3) (lodging-houses); Nurseries and Child-minders Regulation Act, 1948, s.1 (1); Local Government Act, 1972, s.217 (1) (minutes of meetings). The working of the law on admission to meetings and access to information has been the subject of research by A.J. Beith, of Newcastle University Department of Politics.
10. Town and Country Planning Act, 1968, s.3 and s.7
11. H. Lawford, "Privacy versus Freedom of Information", a paper presented at a conference on "Computers: Privacy and Freedom of Information", Queen's University, May 1970
12. Ibid, at p.16
13. C.J. Friedrich, "Secrecy versus Privacy: the Democratic Dilemma", in "Privacy", ed. R. Pennock and J. Chapman, Atherton (N.Y.) 1971, at p.105
14. M.E. McCombs, "Public Access to Computerised Record Systems", ACM 6th Annual Urban Symposium 1971, p.40
15. Departmental Committee on s.2 of the Official Secrets Act, 1911, Cmnd 5104, HMSO, 1972: particularly vol. 1 chapters 6 and 12
16. R.P. Lowry, "Toward a Sociology of Secrecy and Security Systems", 19 Social Problems, pp 437 - 449 at p.449, Spring 1972
17. S. Beer, "Managing Modern Complexity", 2 Futures 245 at 248, September 1970
18. M.B. Jensen, in "Data Banks and Society", Institutt for Privatrett Conference, 1971, Scandinavian University Books, at p.41
19. "The Future of Electronic Computers in Local Government". Report of the proceedings of the First Conference of ICT Computer Study Group, May 1960

20. R.A. Clark, "LOGIC: The Santa Clara County Government Information System and its relationship to the Planning Department", in "Threshold of Planning Information Systems", American Society of Planning Officials, Houston, April 1967. See also Westin (ref (25) below) pp 101 - 110.
21. G. Milliman, "Alameda County's "People Information System"; 13 Datamation p.28, March 1967
22. H. Black, J.E. Shaw, "Detroit's Data Banks", 13 Datamation p.13, March 1967
23. IBM UMIS manuals GE20-0353 to GE20-0371. See also Westin (ref (25) below) pp 89 - 100
24. O.E. Dial, "Why There Are No Urban Information Systems Yet", in A. Westin, "Information Technology in a Democracy", Harvard U.P. 1971, at p.326. Professor Dial seems nevertheless to favour the development of such systems - see Dial, "Misplaced Priorities in Urban Assistance", U.R.I.S.A. 7th Annual Conference, 1969, at p.32
25. A.F. Westin, "Databanks in a Free Society", Quadrangle Books 1972 at pp 236 - 240
26. J.R. Dunn, E. Hearle, "The Wichita Falls Integrated Municipal Information System: Prototype for Cities", in Urban Data Management Symposium, Planning and Transport Research & Computation Co. Ltd., 1972; Dunn, "Status Report on USAC M.I.S. Project in Wichita Falls", U.R.I.S.A. 8th Annual Conference, 1970, at p.46
27. R.D. Hogan (IBM), "Remote Graphical Terminal and Urban Geographical Information System Demonstration", Information Systems Symposium, Washing, 1968.
28. T. Gregory, "The Point Data System ..." Coventry B.C. report. January 1970
29. Tomlinson, Huff, "The Creation of Geo-coded Files", in P.T.R.C. Co. Symposium (see ref (26) above)
30. Stephenson, Younger, "Problems of Introducing a Point Referenced Data System in an Urban Authority", P.T.R.C. Co. Symposium (see ref (26) above).
31. Under phase I of the LAMIS project: "Leeds and ICL join in computer project", Local Government Chronicle, 9 June 1972; Computer Weekly News Report, 8th June 1972, p.1
32. The project has developed from a scheme proposed by Haringey: "London Borough of Haringey Long Term Computer Project . Report on the Initial Study". London Borough's Management Service Unit, 1969

33. E. Cristiani, Evey, Goldman and Mantey, "An Interactive System for Aiding Evaluation of Local Government Policies"; IEEE Transactions on Systems, Man and Cybernetics. March 1973, p.141 at p.142
34. R. Keston, "In search of a City: is Information System Integration Feasible?"; ACM 5th Annual Symposium (Computers and Urban Society) 1970 p.53
35. O. Salomonsson, "Data Banking Systems for Urban Planning", 3 IAG Journal No. 1 (1970) p.23 at p.24; See also: (b) LAMSAC "Computer Development in Local Government", 1969, paras 26, 27: (c) Jakobsen, "Report on the use of computers in local government", Consultative Assembly of the Council of Europe, 1969, para 3.1.5
36. See eg., LAMSAC "A study of the Computing Requirements of Local Government in England", Phase I Report, 1973, p.4
37. M.E. Weiner, "Trends and Directions for Urban Information Systems", in Westin "Information Technology in a Democracy", Harvard U.P. 1971, at p.347
38. A single annual form was proposed in an editorial, New Law Journal, 17th August 1972, at p.738. For this author's criticisms, see NLJ correspondence, 24th August 1972, and Local Government Chronicle 14th April 1972 at p.619
39. C.W. Churchman, "The Use of Science in Public Affairs", in "Governing Urban Society: New Scientific Approaches", Monograph No. 7, American Academy of Political and Social Science, 1967, pp 29 - 48
40. Study Team from Department of Environment et al, "General Information System for Planning", HMSO, 1972
41. Ref (36) above
42. Ibid, at p.18
43. Ibid, at p.3
44. Ibid, at p.24, p.70
45. Ibid, at p.22, p.48
46. Ibid, at p.72
47. Department of Environment et al, "General Information System for Planning", HMSO, 1972, at p.41
48. Ibid, at p.50, p.95
49. Ibid, at p.19, p.26, pp 31 - 35, pp 71 - 73

CHAPTER 5 (continued)

(pages 104 - 117)

50. A. Mindlin, "Confidentiality and Local Information Systems", Public Administration Review. Nov/Dec 1968, pp 509 - 517 at p.514
51. Maud Committee, "Management of Local Government", 1967, at para 233
52. Reports in Local Government Chronicle: 7.6.69, 3.10.70, 11.8.72
53. Reports in Local Government Chronicle: 2.8.69, 30.1.71
54. A. Thorburn, "The East Midlands data bank", LCC 19th July 1969, at p.1327
55. A.E. Phillips, "Joint development of computer programs", Local Government Chronicle, 2 November 1968 p.1745. (All the collaborating authorities were NCR 315 users)
56. LAMSAC, "Local government computer development in Wales, final report of the working party", 1973
57. Report, "The Danish Solution", 13 Data Systems, January 1972, pp 28-30
58. C.W. Mallinson, Proceedings of 1968 A.M.C. Conference (Brighton) at p.36

CHAPTER 6

(pages 120 - 141)

1. "Children in Trouble", Cmnd 3601, HMSO, April 1968
2. J.C. Richardson, "Social Enquiry Reports and the Juvenile Court", 136 Justice of the Peace 74, January 1972
3. Discussion Paper, "Confidentiality in Social Work", British Association of Social Workers, 1971, para 2.11
4. Report of Seminar on new social services departments, Local Government Chronicle, 12th December 1970, p.2497 at 2499
5. Seebohm Committee Report, Cmnd 3703, 1970, at para 300
6. Ibid, at para 466
7. Ibid, at para 426
8. L.N. Robins, "Deviant Children Grown Up", Williams & Wilkes, Baltimore, 1966 (particularly p.32)

CHAPTER 6 (continued)

(pages 120 - 141)

9. See eg., Power, Benn, Morris, "Neighbourhood, School and Juveniles before the Courts", 112 Brit. Jnl. of Criminology, pp 111 - 132, April 1972; Power, Schoenberg, Alderson, "Identifying Persistent Juvenile Offenders" in "The Use of Predictive Methods in Social Work", National Institute for Social Work Training, 1967
10. Interview with Mr. P. Page, Tower Hamlets Courts Section, 5th March 1973
11. Seebohm Committee (ref (5)) para 590

CHAPTER 7 (continued)

(pages 142 - 163)

1. D. Yates, "Security of Tenure and Council House Tenants", New Law Journal 9th November 1972, p.983
2. J.B. Rule, "Private Lives and Public Surveillance", Allen Lane, 1973, chapter 4.
3. LAMSAC Computer Panel, "Towards a Total Housing System", LAMSAC 1972
4. Central Housing Advisory Committee, "Council Housing: Purposes, Procedures and Priorities", HMSO, 1969, at p.30 and p.124
5. J.M. Carroll, J. Baudot, C. Kirsh, J. Williams, "Personal Records: Procedures Practices and Problems" (study commissioned by Dept of Justice), Ottawa, 1972

CHAPTER 8

(pages 176 - 185)

1. IBM Manual E20-0329-0 "System/360 Data Processing in the City of Memphis School System"
2. "Computer Monitors Hooky Players in Michigan Schools", Datamation, April 1969, p.179
3. Form C 10 M, Gloucestershire County Council
4. H. Strasburg, R. Cooney, E. Guliani, "Computer Assisted Instruction", undated, Sperry Univac, London
5. Preface to reference (1) above
6. Central Advisory Council for Education, "Half our Future", HMSO, 1963, chapter 21

CHAPTER 8 (continued)

(pages 176 - 185)

7. Joint research project, IEM Scientific Centre and Cheshire County Council
8. J.W. Ramey, "Urban Data Banks and the Rights of the Individual", 1 Socio-Economic Planning Science, 1968, pp 327 - 333

CHAPTER 9

(pages 186 - 196)

1. F. Stephenson, "Solving the problems of a great city", Computer Weekly 16 December 1971, p.9

CHAPTER 11

(pages 201 - 217)

1. W. May, S. Czecha, "Trade off Analysis between Centralised and Decentralised Network Design", Computer Systems Design '72 West Conference, Anaheim, February 1972 at pp 81 - 89; but see A.G. Mollegaard, "Centralisation versus Decentralization of EDP Functions in Government", World Conference on Information in Government, October 1972 at p.494
2. The need for indenture of deeds was abolished by s.5 of the Real Property Act, 1845 (since consolidated in the Law of Property Act, 1925, s.56)
3. NASA, Handbook for Contamination Control on the Apollo Program, 1966.
4. A. Hawker, "Privtype: a proposal for the control of personal information", Datafair 73, Vol.1, p.82
5. T.D. Friedman, "The authorisation problem in shared files", IEM Systems Journal, No. 4, 1970, pp 258 - 281.
6. L.J. Hoffman, "The Formulary model for access control and privacy in computer systems", U.S.A.E.C. Report, SLAC-117, May 1970

CHAPTER 12

(pages 218 - 247)

1. See eg., J.W. Ramey, "Urban Data Banks and the Rights of the Individual", *Socio-Economic Planning Science*, Vol. 1, pp 327 - 33 (1968) at p.332; J. Jacob, "Data Banks, The Computer, Privacy and the Law", *N.C.C.L.* 1968 at p.12; B.J.A. Hargreaves, "Mass Communications, Technology and the Individual", *IBM* 1968 at p.15; L. Huckfield, *Hansard* vol. 822, col. 495, 27 July 1971 (and in the Bills he has sponsored); R.P. Henderson, "Computers and Privacy", *S.A.M. Advanced Management Journal* July 1971, at p.8
2. Fair Credit Reporting Act, (Public Law 91 - 508, Title VI of Consumer Credit Protection Act), 1970, s.609
3. Data Act, Stockholm, May 11th 1973, s.10
4. Control of Personal Information Bill, 1972, clause 6(7)
5. Privacy Committee of the BCS, "Submission of evidence to the committee on privacy", *Computer Bulletin* May 1971 at p.176
6. Report of the Committee on Privacy, Cmnd 5012, 1972, para 621
7. No definitive commitment has been made, but the idea of a commission was to be considered along with other Younger Committee proposals, in the White Paper promised for 1973. See: *Hansard*, 13th July 1973, col. 1967, and *Hansard (H.L.)* 6th June 1973, col. 172.
8. Younger Committee report (ref. 6, supra) para 612
9. Ref. 4 supra, clauses 6(1) and 6(5)
10. Cf Younger Committee report at para 605
11. BCS Privacy and Public Welfare Committee, "Privacy and the Computer - Steps to Practicality", 1972, at p.13
12. Younger Committee report para 610
13. Y. Dror, "Law and Social Change", in Aubert, "Sociology of Law". Penguin, 1969, p.90
14. LAMSAC, "Computer Privacy - Notes of Guidance for Local Authorities", 1972

CHAPTER 13

(pages 248 - 253)

1. T.A. Cowan, "Decision Theory in Law, Science and Technology", *140 Science*, June 7th 1963, pp 1065 - 1075
2. J.B. Rule, "Private Lives and Public Surveillance", Allen Lane, 1973, p.164

GLOSSARY

* denotes words used in a special sense in the thesis

A.C.M.	Association for Computing Machinery (USA)
B.C.S.	British Computer Society
* CLAIM	Usually meaning a proper or justifiable claim. See introduction
* COLLECTOR	Someone at the interface between the system and the outside world who is responsible for putting data into the system. (Chapter 2)
CONFIDENCE	In Law, an equitable remedy (Chapter 3)
CONFIDENTIALITY	Based on a presumption that information is not to be disclosed, because of personal obligation or administrative directives; but not an absolute restriction (compare SECRECY)
* CONTEXT-DATA	Data relating to circumstances surrounding the INDID-DATA (Chapter 2)
CONTROL	1. Social control. Encouraging or enforcing certain kinds of behaviour 2. Computing. Issuance of instructions from privileged programs
DATABANK	Any large collection of data, however organised
DATABASE	A large collection of data so organised that each data item is stored, as a rule, only once, and with a freedom from structures imposed on it such that any number of user's programs can operate on the same data
DISCOVERY	In Law, procedure for obtaining documents from the other side prior to trial
* DIVULGED	Of information, any personal information obtained with the knowledge of the indid (Chapter 2)
* HOLDER	Someone responsible for the operation of a databank (Chapter 2)
* INDENTURE-DATA	Data necessary to link names or other identifying data to indid-data stored in a computer system (Chapter 11)

* INDID	The <u>individual identified</u> in a data item or record
* INDID-DATA	The data relating to an indid
L.A.M.S.A.C.	Local Authorities Management Services and Computer Committee
MACRO	In Computing, a program which can be invoked to carry out some standard procedure
* OBSERVED	Of information, <u>not</u> obtained with the knowledge of the indid (cf DIVULGED)
* PRIVACY	A claim to be allowed autonomy, and freedom from observation and surveillance. Very wide-ranging, and little agreement on precise definitions. In this thesis, restricted to the claim to influence decisions whereby information is made available to other people.
PRIVILEGE	<ol style="list-style-type: none"> 1. Legal - a right to keep information secret (e.g., legal professional privilege), or a right to make statements without fear of the consequences. The latter may be "qualified" i.e., you lose the protection by being malicious. 2. Computing - of programs, pertaining to an ability to direct or control other programs.
* PRIVTYPE	A privacy label. See Chapter 11
READ	In Computing, an operation whereby data is read from a tape or disc and made available in the central processing unit (cf WRITE)
RIGHT	Something to which someone is entitled, usually under the terms of the Law, in prescribed circumstances
SECRECY	An absolute prohibition on disclosure of information
SURVEILLANCE	The maintenance of current or historical facts relating to a large number of people in a databank
* SYSTEM INNUENDO	A particular interpretation of systematically stored data, which is widely known to users of the system (Chapter 3)
* USER	Someone who can readily obtain data from a databank, whether directly or through an intermediary (Chapter 2)
WORD	In Computing, a grouping of about 24 bits (depending on machine type). Will carry about four characters
WRITE	In Computing, an operation whereby data is transferred from the central processing unit to a storage device such as tape or disc.

APPENDIX IOFFICIAL INVESTIGATIONS IN THE U.S.A.

Over the past decade, numerous studies and hearings have taken place under the auspices of the United States Federal Government.

A summary of these investigations, in chronological order, is given below. For more detailed references, the reader is referred to A.R. Miller, "The Assault on Privacy", University of Michigan Press, (1971) at p.271.

<u>Subject</u>	<u>Investigating Body</u>	<u>Date</u>
Government Agencies	SAPAP	1965, 1966
Special Inquiry, Privacy	SC	1965 - 1967
Computers	SC	1966
Computers	SAPAP	1967
Federal Employees	CRS	1967
Federal Employees	COJ	1967
Right of Privacy Act	SAPAP	1967
National data bank	CGO	1968
Credit Bureaux	SC	1968
Computers	SAPAP	1968
Government dossier	SAPAP	1968
Credit Industry	SAM	1969
Federal Employees	SMCS	1969
Federal Employees	COJ	1970
Census	CPO	1970

Interpretation:

CGO	Committee on Government Operations
COJ	Committee of the Judiciary
CPO	Committee on Post Office & Civil Service
CRS	Constitutional Rights Subcommittee
SAM	Subcommittee on Antitrust & Monopoly
SAPAP	Subcommittee on Administrative Practice and Procedure
SC	Special Subcommittee (no title)
SMCS	Subcommittee on Manpower and the Civil Service

All the investigations were concerned specifically with the privacy aspects of the subjects mentioned.

APPENDIX II

AREAL UNITS IN BIRMINGHAM

Housing Department,
City of Birmingham.
(source: sketch from
wall map in Bush House)



Supplementary Benefits
(source: DHSS listing
by postcode areas)

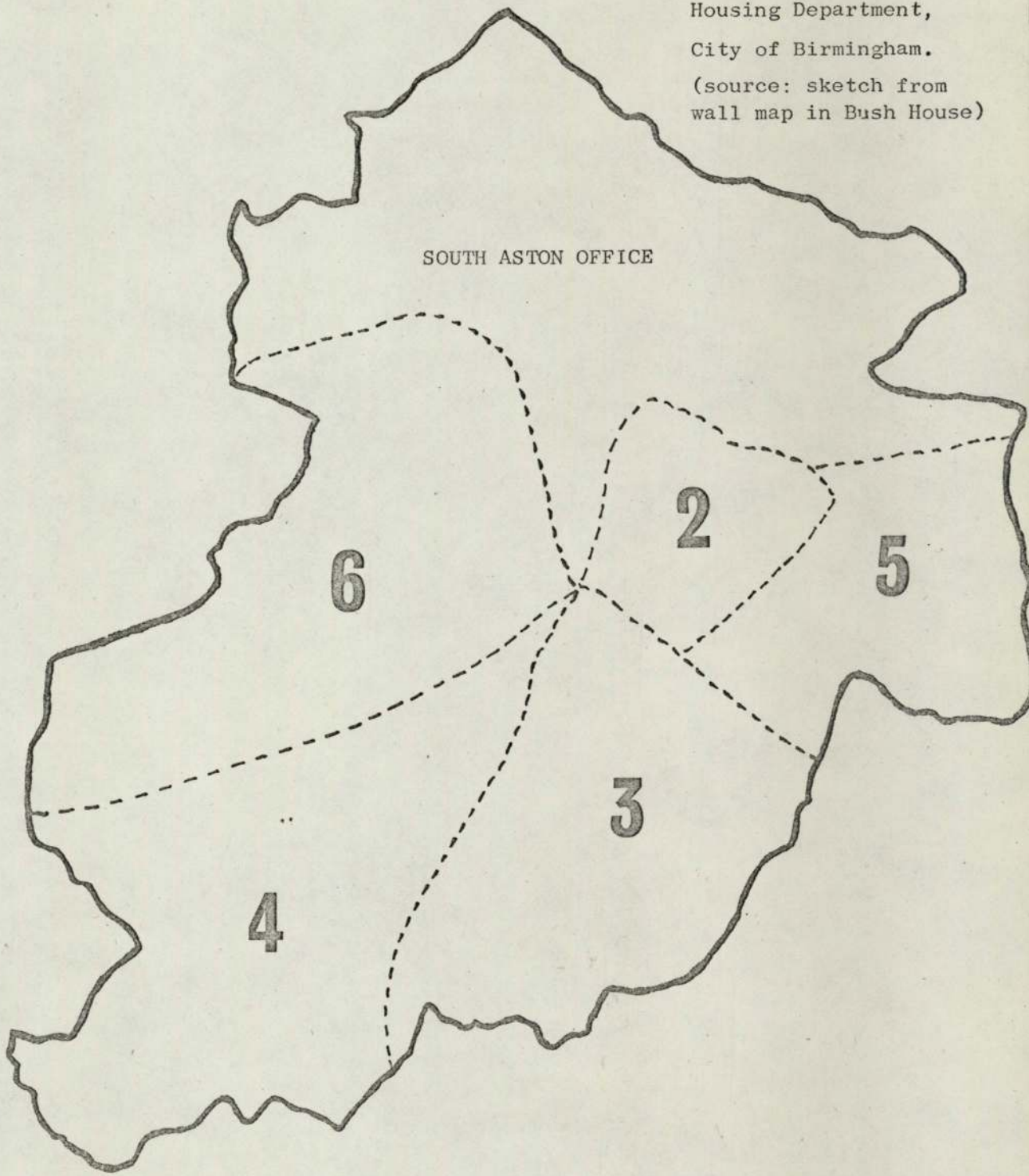


Housing Department,
City of Birmingham.
(source: sketch from
wall map in Bush House)



Social Services Department,
City of Birmingham.
(source: S.S.D. listing
by Ward Boundaries)

Housing Department,
City of Birmingham.
(source: sketch from
wall map in Bush House)



SOUTH ASTON OFFICE

6

2

5

3

4

City of Birmingham
(source: S.S.D. Listing
by Ward Boundaries)

APPENDIX IIISample privtype transactions

(1) Input via a terminal. The conversation might appear like this:-

(* denotes system messages. The user's responses are underlined)

* privtype: automatic? (Y/N)

N

* privtype default codes are:

1. identity of collector 06115 33 27
2. data not to be passed to NIL
3. reliability of the data GOOD
4. reliability will continue MONTH
5. data should be retained YEAR
6. individual requested confidence NO
7. someone else requested confidence NO

* Key number(s) of code(s) to be altered,

* separating by commas. If no alteration, key 9

2, 6

* 2. Values are: SPOUSE, PARENT, CHILD, CLOSE, EMPLOYER, NIL
For further explanation, Key 9 and value.

9 CLOSE

* CLOSE means that a friend, neighbour, or relative

* (apart from spouse, parent or child) ought not to be

* given the information

NIL

* 6. Values are: V.HIGH, MEDIUM, LOW

V.HIGH

* Start data entry

Note: the collector would not have to go through this procedure for

repetitive data entry. If he was familiar with the default codings, he could authorise their association with the data by simply replying "Y" to the question "privtype: automatic?". The system would of course be able to deduce the collector-code from the logging procedure.

- (2) Input on documents. An advisory document might be issued to all staff, as follows:-

Midshire County Council

Storage of Personal Information

Under the Personal Information Act, 1977, the County Council must ensure that computer-based information is handled responsibly. All staff members, as "collectors" of data, are responsible for deciding on codings which will affect the later circulation and use of data.

Usually, "default" values of these codings will have been agreed for your section. However, you may change the coding for any data where you are the collector of it. The values of the codings, whether they are changed or whether they stay at the default values, are your responsibility.

On input documents, you will find fields as follows:-

COLLECTOR

--	--	--	--	--	--	--	--	--	--

DEFAULT PRIVTYPE	A	B	C	D	E	F
	Not to	Reliable	Cont's	Retain	Confidence	
	NIL	GOOD	YEAR	YEAR	NO	NO

By each data item, a further field appears:

--	--	--	--

Suppose you wish to enter different values from those in the default privtype: for example, you wish to indicate that the data will be reliable only for a month, and that the person supplying the data particularly stressed that it was given in confidence.

You should enter next to that data:

C	MONTH	E	V.HIGH
---	-------	---	--------

A full explanation of the codings permitted, and their meanings and functions, is given below.

(Simple statements on the nature of each privtype coding would then follow).

BIBLIOGRAPHY

1. B. Allen, Danger Ahead! Safeguard Your Computer.
Harvard Business Review, Volume 46, Page 97, November 1968
2. Anon, News Item, Computer Monitors Hooky Players in Michigan Schools.
Datamation, Volume 15, Page 179, April 1969
3. Anon, Computers in Central Government: Ten Years Ahead.
(particular Chapter 4)
CSD Management Studies 2 (HMSO) 1971
4. Anon, Confidentiality in Social Work. Report of a Working Party.
British Association Social Workers, London, 1971
5. Anon, The Consideration Of Data Security In A Computer Environment.
IBM 821 UN Plaza New York NY10017, 1969
6. Anon, Data Security in the Corporate Data Base.
EDP Analyzer, Volume 8, page 1, May 1970
7. Anon (News Item), Emerging Tort of Intrusion.
IOWA Law Review, Volume 55, page 718, February 1970
8. Anon (News Item), IBM Goes Public on Computer Privacy.
New Scientist, page 628, 10th June 1971
9. Anon, Landmark Study of Computer-Privacy Problem Completed
(Westin Report)
Communications of the ACM, Volume 15, page 1096, December 1972
10. Anon, London Borough of Haringey Long Term Computer Project:
Initial Study.
London Boroughs' Management Services Unit, 1969
11. Anon, Measures to Protect Personal Privacy Increase at State Level
Communications of the ACM, Volume 16, page 65, January 1973
12. Anon, 1904S for CSD Databank Project
Computer Weekly, page 1, 5th October 1972
13. Anon (News Item), Physician-Patient Confidences: Legal Effects of
Computerization of Records.
Alabama Lawyer, Volume 31, page 393, April 1970
14. Anon, Privacy and Efficient Government: Proposals for a National
Data Centre.
Harvard Law Review, Volume 82, page 400, December 1968
15. Anon, Project - The Computerization of Government Files: What
Impact on the Individual?
U.C.L.A. Law Review, Volume 15, page 1371, September 1968

16. Anon, Remarks on the Question of Privacy Raised by the Automation of Mental Health Records.
Rand Corporation, P-3523, April 1967
17. Anon, The Right to Privacy in Canada.
Faculty of Law Review of University of Toronto,
Volume 25, page 103, May 1967
18. Anon, Speak Out: Privacy Under Threat.
NCCL, 152 Camden High Street, London NW1, 1969
19. Anon (News Item), Suspension of Employee on Basis of Information in Confidential Report obtained by Employer.
Wayne Law Review, Volume 16, page 339, 1969
20. J.D. Babcock, A Brief Description of Privacy Measures in the "RUSH" Time-Sharing System.
AFIPS Proc Spring J'P Comp Conf P 301, 1967
21. R. Bachi, R. Baron, Confidentiality Problems Related to Data Banks.
International Statistics Institute, Paper BA18 September 1969
22. P. Baran, On Distributed Communications: 9, Security Secrecy and Tamper-Free Considerations.
Rand Corporation, RM-3765-PR, August 1964
23. P. Bartram, Wild West Sussex System
Dataweek, page 12, 18th March 1970
24. W.S. Bates, Security of Computer-Based Information Systems.
Datamation, Volume 16, page 60, May 1970
25. BCS, Royal Statistical Society, Security of the Census of Population
HMSO, (Cmnd 5365) 1973
26. BCS Privacy Committee, Privacy and the Computer: Steps to Practicality. BCS, 29 Portland Place, W.1. 1972
27. BCS Privacy Committee, Younger Report, A Review
BCS Computer Bulletin, Volume 16, page 455, September 1972
28. W.M. Beaney, The Right to Privacy and American Law.
Law & Contemporary Problems, Volume 31, page 253, April 1966
29. S. Beer, Managing Modern Complexity - 1.
Futures (IPC Business Press) Volume 2, page 114, June 1970
30. S. Beer, Managing Modern Complexity - 2.
Futures (IPC Business Press) Volume 2, page 245, September 1970
31. H.W. Bingham, Security Techniques for EDP of Multilevel Classified Information. (Coded RADC-TR-65-415)
Griffiths Air Force Base, N.Y. 1965
32. H. Black, E. Shaw, Detroit's Data Banks,
Datamation, Volume 13, page 25, March 1967

33. R.F. Boruch, Education Research and the Confidentiality of Data
American Council of Edn, Volume 4, No. 4, 1969
34. K.E. Bodenham, F. Wellman, Review of Foundations of Health
Service Management.
Nuffield Prov Hosp Trust/Oxf Univ Pr, 1972
35. L.D. Brandeis, S. Warren, The Right to Privacy.
Harvard Law Review, Volume 4, page 193, 1890
36. L. Brittan, The Right of Privacy in England and the United States.
Tulane Law Review, Volume 37, page 2235, 1962
37. V.B. Brown, W. Mason, M. Kaczmariski,
A Computerised Health Information Service.
Nursing Outlook (N.Y.) Volume 19, page 158, March 1971
38. Buchan, Written Question, Information Exchange Between Government
Departments.
Hansard, Volume 847, page 228, 29th November 1972
39. Byers, Lord et al, Debate on Younger Committee Report.
Hansard (H.L.), Volume 343, page 104, 6th June 1973
40. J. Callaghan, Membership of Younger Committee - Written Reply.
Hansard, Volume 799, page 270, 16th April 1971
41. R. Carr et al, Debate on Younger Committee Report.
Hansard, Volume 859, page 1955, 13th July 1973
42. J.M. Carroll, Baudot, C. Kirsh,
Personal Records: Procedures, Practices and Problems.
Information Canada, Ottawa, 1972
43. Chronicler (News Item), Keeping a Check on Computers.
Local Government Chronicle, page 280, 18th February 1972
44. H.S. Conrad, Clearance of Questionnaires with Respect to "Invasion
of Privacy" Public Sensitivities, Ethical Standards, etc.
American Psychologist, Volume 22, page 356, May 1967
45. Chronicler (News Item), Confidentiality and its Limitations
Local Government Chronicle, page 142, 23rd January 1971
46. E.V. Comber, Management of Confidential Information.
p135ACM Fall Jt Computer Conference 1969
47. R.W. Conway, W.L. Maxwell, H.L. Morgan
On the Implementation of Security Measures in Information Systems
Communications of the ACM, Volume 15, page 211, April 1972
48. W.A. Creech, The Privacy of Government Employees.
Law & Contemporary Problems, Volume 31, page 413, April 1966
49. W.J. Curran, B. Stearns, H. Kaplan, Privacy Confidentiality &
Other Legal Considerations (for Health-Data System)
New England J of Medicine, 31 July 1969

50. A. D'Agapeyeff, E. Willey, G. Morris, Sub-Committee "A" Evidence. HMSO (Ref. 267-XI), 1971
51. A. D'Agapeyeff, The Data-to-Data Check
The Guardian, page 12, 20th May 1971
52. W.P. Davey, Local Government Computer Development in Wales.
Computer Bulletin (BCS) December 1969
53. M. Davies, Toward a Medical Data Bank for a Total Population.
Datamation, Volume 15, page 257, November 1969
54. F.G. Debalogh, Public Administrators and the Privacy Thing: A Time
to Speak Out.
Public Administration Review, page 526, September 1972
55. R.L. Dennis, W. Ware, J. Russell, R. Von Buelow,
Security in the Computer Environment.
Systems Development Corporation Conference, August 1966
56. Department of Justice, Privacy and Computers: Report of Task Force.
Information Canada, Ottawa, 1972
57. C. Fanwick, Maintaining Privacy of Computerized Data.
Systems Development Corporation, SP-2647, December 1966
58. M.A. Farr, B. Chadwick, K.K. Wong, Security for Computer Systems.
National Computing Centre, 1972
59. W.V. Fogler, G. Benjamin, Applying Com to a Job Bank.
Datamation, Volume 15, page 112, December 1969
60. D. Foulkes, Local Authorities and Official Secrets.
Local Government Chronicle, page 1080, 12th October 1973.
61. R.G. Fox, Professional Confidences and the Psychologist.
Tasmania University Law Review, Volume 3, page 12, December 1968
62. N. Foy, A Bonfire of Census Forms.
New Scientist, page 132, 15th April 1971
63. A.G. Fraser, User Control in a Multi-Access System.
BCS Computer Journal, Volume 11, page 12, 1968
64. C. Fried, Privacy.
Yale Law Journal, Volume 77, page 475, 1968
65. T.D. Friedman, The Authorisation Problem in Shared Files
IBM Systems Journal, page 258, November 1970
66. E.R. Gabrieli, Right of Privacy and Medical Computing.
Datamation, Volume 16, page 173, April 1970
67. E.R. Gabrieli, Medical Network.
Datamation, Volume 16, page 42, May 1970

68. R.R. Gallati, Criminal Justice Systems and the Right to Privacy.
5th Annual Conference
Urban & Regional Infn Syst Assn, 1967
69. H.P. Gassman, Data Banks and Individual Privacy: Situation in
Germany.
Computer Communication Conference (ACM, IEEE) 1972
70. C.C. Gotlieb, J.N. Hume, Systems Capacity for Data Security
Information Canada, Ottawa, 1972
71. C.C. Gotlieb, Regulations for Information Systems.
Computers and Automation, page 14, September 1970
72. R.M. Graham, Protection in an Information Processing Utility.
Communications of the ACM, Volume 11, page 365, May 1968.
73. M. Greenberger, Computers, Communications and the Public Interest.
(particularly chapter 5)
John Hopkins Press, 1971
74. E.J. Grenier, Jr, Computers and Privacy: A Proposal for Self-
Regulation.
Duke Law Journal, page 495, 1970
75. R.F. Guise, File Security.
Data Systems News, Volume 10, page 60, November 1969
76. Gutteridge, Walton, The Comparative Law of the Right of Privacy.
Law Quarterly Review, Volume 47, page 203, 1931
77. "T.H.", Privacy, The Press and Mrs. X.
New Law Journal, page 666, 20th July 1972
78. P. Hamilton, Computer Security.
Cassell, 1972
79. J.F. Handler, E.J. Hollingworth,
Stigma, Privacy and Other Attitudes of Welfare Recipients.
Stanford Law Review, Volume 22, page 1, November 1969
80. J.F. Handler, M. Rosenheim,
Privacy in Welfare, Public Assistance and Juvenile Justice.
Law & Contemporary Problems, Volume 31, page 377, April 1966
81. M.H. Hansen, Insuring Confidentiality of Individual
Fall Joint Computer Conference, AFIPS, p579, 1971
82. B.J. Hargreaves, Mass Communications Technology and the Individual
(IBM) 22nd Ramsay Muir Lecture, Nottingham University, 1968
83. A.E. Harum, Right of Privacy in Europe.
Antitrust Law Journal, Volume 56, page 673, July 1970
84. P. Harvey, Commercial Spies Tap State Records.
The Guardian, page 1, 11th May 1971

85. J.J. Hellman, Privacy and Information Systems - An Argument and an Implementation.
Rand Corporation P-4298, May 1970.
86. G.E. Hemmings, Privacy in the Database Environment,
Datafair 73, Volume 1, B.C.S. page 70, 1973
87. R.P. Henderson, Computers and Privacy.
S.A.M. Adv. Management Journal, Volume 36 page 8, July 1971
88. R. Henderson, Controlling the Computer's Threat to Privacy.
Michigan Business Review, Volume 23, page 9, November 1971
89. P. Hirsch, Computer Systems and the Issue of Privacy.
Datamation, page 90, December 1972
90. L.J. Hoffman, Computers and Privacy: A Survey.
Computing Surveys, Volume 1, page 85, June 1969
91. L.J. Hoffman, W.F. Miller,
Getting a Personal Dossier from a Statistical Data Bank.
Volume 16, page 74, May 1970
92. L.J. Hoffman, Security and Privacy in Computer Systems.
(Incorporates other References, including 22 above)
John Wiley, 1973
93. D.K. Hsaio, A File System for a Problem Solving Facility (PhD Thesis)
University of Pennsylvania, 1968
94. L. Huckfield, Databanks in the Administration of Government -
House of Commons Debate.
Hansard, Volume 882, page 487, 27th July 1971
95. L. Huckfield, First Reading of Control of Personal Information Bill.
Hansard, Volume 830, page 1139, 8th February 1972
96. L. Huckfield, Debate on Control of Personal Information Bill.
Hansard, Volume 835, page 967, 21st April 1972
97. L. Huckfield, NCC Project for LEA Data, Adjournment Debate.
Hansard, Volume 819 page 948, 18th June 1971
98. L. Huckfield, Oral Question: DES Research on Computer Records in
Schools.
Hansard, Volume 834, page 1412, 13th April 1972
99. L. Huckfield, Written Question: to Mrs. Thatcher: Local Authority
Records.
Hansard, Volume 820, page 425, 8th July 1971.
100. P. Jackson, Privilege and the Public Interest.
Local Government Chronicle, page 1108, 19th October 1973.
101. J. Jacob, Academic Freedom and the Law - Appendix 5.
NCCL, 186 Kings Cross Road, WC1., 1971

102. J.M. Jacob, A New Attempt to Control Data Banks.
Law Guardian, Volume 68, page 19, April 1971
103. J. Jacob, Data Banks, The Computer, Privacy and the Law.
NCCL, 152 Camden High Street, NW1. 1969
104. J. Jacob, R. Jacob, Confidential Communications.
New Law Journal, Volume 119, page 133, February 1969
105. Justice, Living it Down - The Problem of Old Convictions.
Stevens, 1972
106. Justice, Privacy and the Law.
Stevens & Sons Ltd., London, 1970
107. S.M. Jourard, Some Psychological Aspects of Privacy.
Law & Contemporary Problems, Volume 31, page 307, April 1966.
108. H. Kalven, Privacy in Tort Law: Were Warren and Brandeis Wrong?
Law & Contemporary Problems, Volume 31, page 326, April 1966
109. K.L. Karst, "The Files": Legal Controls over the Accuracy and
Accessibility of Stored Personal Data.
Law & Contemporary Problems, Volume 31, Page 342, April 1966
110. C. Kaysen, Report of Task Force on Storage of and Access to
Government Statistics.
Bureau of the Budget, USA, 1966
111. H. Keast, Confidentiality in Local Services.
Local Government Chronicle, page 1222, 10th July 1971.
112. M.R. Konvitz, Privacy and the Law: A Philosophical Prelude.
Law & Contemporary Problems, Volume 31, page 272, April 1966
113. T.D. Kuch, "ANSI" Identification (Standard for identification of
individuals).
Datamation, Volume 17, page 52, January 1971
114. LAMSAC Computer Panel, Computer Installations in Local Government.
LAMSAC, 35 Belgrave Square, SW1, December 1972
115. R.E. Leeves, Problems of Confidentiality.
Case Conference (Journal), Volume 14, page 371, February 1968
116. K. Lenk, M.B. Jensen, G.R. Pipe, Data Banks and Society.
Universitetsforlaget, Oslo, 1972
117. R.P. Lowry, Toward a Sociology of Secrecy and Security Systems.
Social Problems, page 19, May 1972
118. L. Lusky, Invasion of Privacy, A Clarification of Concepts.
Political Science Quarterly, Volume 87, page 192, June 1972
119. D. Madgwick, Privacy Under Attack.
NCCL, 186 Kings Cross Road, WCL, 1968

120. C.W. Mallinson, Computer Development in West Sussex, Local Government Chronicle, page 1581, 23rd August 1969
121. J. Martin, A.R. Norman, The Computerised Society. Prentice-Hall Inc. 1970
122. S.L. Mathison, P.M. Walker, Computers and Telecommunications: Issues in Public Policy. Prentice-Hall Inc. 1970
123. H. Matusow, The Beast of Business: A Record of Computer Atrocities. Wolfe Publishing Ltd, London, 1968
124. B. Meek (ED), Computers and the Year 2000. (particularly chapter 20 on Privacy) National Computing Centre, 1973
125. A.R. Miller, The Assault on Privacy. University of Michigan Press, 1971
126. A.R. Miller, Personal Privacy in the Computer Age: The Challenge of a New Technology. Michigan Law Review, Volume 67, page 1091, April 1969
127. A.R. Miller, The National Data Centre and Personal Privacy. Atlantic Monthly, December 1967
128. A.R. Miller, Federal Data Banks and the Bill of Rights. Computers and Automation, page 12, 1971
129. A.R. Miller, J.D. Pemberton, R. Ruggles, Symposium: Computers, Data Banks and Individual Privacy. Minnesota Law Review, Volume 53, page 211, December 1968.
130. G. Milliman, Alameda County's "People Information System". Datamation, Volume 13, page 28, March 1967
131. A. Mindlin, Confidentiality and Local Information Systems. Public Administration Review, page 509, November 1968
132. J. Moss, Confidentiality and Identity. Lockheed Gout Inf Syst Rept GIS-83, 1968
133. M. Murch, Privacy - No Concern of Social Work? Social Work Today, Volume 2, page 6, 3rd June 1971
134. E. Myers, Head Hunting by Computer - The Bugs are There but so are the Dollars. Datamation, Volume 16, page 169, May 1970
135. R. Nader, Freedom from Information, The Act and The Agencies. Harvard Civil Rights - Civil Liberties Law Review, Volume 5, page 1, January 1970
136. G. Negley, Philosophical Views on the Value of Privacy. Law & Contemporary Problems, Volume 31, page 319, April 1966

137. Neill, Protection of Privacy.
Modern Law Review, Volume 25, page 393, 1962
138. F.H. Newark, Review of Westin's "Privacy & Freedom".
Law Quarterly Review, Volume 87, page 264, April 1971
139. G.B. Niblett, Computers and Privacy.
BCS Computer Bulletin, Volume 13, page 431, December 1969
140. G.B. Niblett, Data Banks and Individual Privacy: Developments
in the U.K.
Computer Communication Conference (ACM:IEEE) 1972
141. G.B. Niblett, Digital Information and the Privacy Problem.
OECD Informatics Studies, September 1971
142. C. O'Grady, Daring and Ambitious LOLA.
Local Government Chronicle, page 196, 30th January 1971
143. C. O'Grady, Is Your Computer Room Secure?
Local Government Chronicle, page 1241, 21st July 1972
144. D.B. Parker, Privacy in Resource-Sharing Computer Systems.
Control Data Corporation, TER-06, November 1967
145. P.L. Peck, Achieving Security and Privacy of Information in an
On-Line DP Environment.
On-Line 72, Proceedings, page 107, 1972
146. J.R. Pennock, J.W. Chapman, Privacy.
Atherton Press, New York, 1971
147. H.E. Petersen, R. Turn, System Implications of Information Privacy.
AFIPS Proc Spring Jt Comp Conf, page 291, 1967
148. H.E. Petersen, R. Turn, Security of Computerized Information
Systems.
Rand Corporation P-4405, July 1970
149. J.W. Ramey, Computer Information Sharing: Threat to Individual
Freedom.
ADI Convention, October 1967
150. N.J. Ream, The Computer and its Impact on Public Organisation.
Public Administration Review, page 494, November 1968
151. A.C. Richter, Geo-Coding - An Application in a Local Government
Information System.
ACM National Conference Proceedings, 1968
152. J. Rose (ED), Technological Injury. (particularly chapter 10)
Gordon and Breach Science Publishers, 1969
153. J.E. Rule, Private Lives and Public Surveillance.
Allen Lane, 1973

154. E.F. Ryan, The Protection of Privacy in Ontario.
Ontario Law Reform Commission, 1968
155. J. Sawyer, H. Schechter, Computers, Privacy and the National
Data Center.
American Psychologist, Volume 23, page 810, 1968
156. E.S. Selmer, Registration Numbers in Norway: Some Applied
Number Theory and Psychology.
Royal Statistical Society Journal A, Volume 130 page 225, 1967
157. E. Shils, Privacy, Its Constitution and Vicissitudes.
Law & Contemporary Problems, Volume 31, page 281, April 1966
158. T.R. Sizer, Privacy and The Computer.
BCS Computer Bulletin, Volume 16, page 384, August 1972
159. T.R. Sizer, Questionnaire on Privacy and the Computer.
British Computer Society, 1973
160. R.O. Skatrud, A consideration of the Application of Cryptographic
Techniques to Data Processing.
Fall ACM Fall Jt Computer Conference, 1969
161. M. Spiers, The Computer and The Machinery of Government.
Public Administration, Volume 46, page 411, November 1968
162. M.G. Stone, Computer Privacy.
ANBAR Monograph, 1968
163. M.G. Stone, A Matter of Privacy.
Data Management, page 13, January 1971
164. H. Street, The Officer who Gives Away Information.
Local Government Chronicle, page 647, 22nd June 1973
165. B. Sundgren, Security and Privacy in Statistical Databases.
Swedish Bureau of Statistics, 1972
166. C. Tapper, Computers and the Law.
Weidenfeld and Nicolson, 1973
167. G.D. Taylor, Privacy and the Public.
Modern Law Review, Volume 34, page 288, May 1971
168. D. Van Tassel, The Computer vs Privacy.
Law and Computer Technology, Volume 3, page 2, January 1970
169. E. Van Tassel, Computer Security Management.
Prentice-Hall, 1972.
170. Various, The Computer and Invasion of Privacy:
Data Center Hearings
Arno Press, New York, 1967
171. C.W. Vorlander, Data Processing System for Local Government.
Municipality, Volume 60, page 195, August 1965

172. B. Walden, Right of Privacy Bill: Debate on Second Reading.
(Younger Committee C941)
Hansard, Volume 794, page 861, 23rd January 1971
173. W.H. Ware, Security and Privacy: Similarities and Differences.
AFIPS Proc Spring Jt Comp Conf page 287, 1967
174. W.H. Ware, Computer Data Banks and Security Controls.
Rand Corporation P-4329, March 1970
175. W.H. Ware, Security and Privacy in Computer Systems.
AFIPS Proc Spring Jt Comp Conf page 279, 1967
176. M. Warner, G. Peters, The Data Bank Dilemma.
Local Government Chronicle, page 835, 10th May 1969.
177. M. Warner, M. Stone, The Data Bank Society.
George Allen & Unwin, 1970
178. C. Weissman, Programming Protection: What Do You Want To Pay?
Systems Development Corporation Magazine, Volume 10, page
August 1967
179. C. Weissman, Security Controls in the ADEPT-50 Time-Sharing
System.
Pl19 ACM Fall Jt Computer Conference 1969
180. A.F. Westin, Computers and the Protection of Privacy.
Technology Review, page 32, April 1969
181. A.F. Westin, M.A. Baker, Databanks in a Free Society.
Quadrangle Books, 330 Madison Avenue, N.Y. 1972
182. A.F. Westin, Information Technology in a Democracy
Harvard University Press, 1971
183. A.F. Westin, Life, Liberty and the Pursuit of Privacy.
Think (IBM) Volume 35, page 12, May 1969
184. A.F. Westin, New Laws Will Protect Your Privacy.
Think (IBM) Volume 35, page 27, May 1969
185. A.F. Westin, Privacy and Freedom.
Bodley Head (Atheneum in USA) 1970
186. A.F. Westin, Privacy: The Basic Questions to be Faced are
Political, not Technical. (Speech at Brookings Institution)
Datamation, Volume 16, page 161, February 1970
187. G. Whitear, Privacy and the Computer.
New Law Journal, page 555, 22nd June 1972
188. P. Winfield, Privacy.
Law Quarterly Review, Volume 47, page 23, 1931
189. Working Party, Data Collection and Privacy.
Social & Comm. Planning Research London, 1972
190. K. Younger, Report of the Committee on Privacy.
HMSO, Cmnd 5012, July 1972

INDEX TO CASES

	Page
Ackroyds v Islington Plastics (1962)	47
Adam v Ward (1917)	58
Addis v Gramophone Co. (1909)	58
Allsop v Church of England Newspaper (1972)	65
Angel v H.H. Bushell (1968)	59
Argyll v Argyll (1967)	53, 55
Ashburton v Pape (1913)	78, 238
Att-Gen v Mulholland (1963)	78
Baker v Carrick (1894)	59
Baker v Gibbons (1972)	50
Balden v Shorter (1933)	58
Barnett v Allen (1858)	65
Barr v Musselburgh Merchants Association (1912)	62
Beach v Freeson (1971)	59
Beatson v Skene (1860)	79
Bennett v Brumfitt (1867)	75
Bleakley v Smith (1840)	74
Bluck v Gompertz (1852)	75
Bottomley v F.W. Woolworth (1932)	64
Bradstreets Britain Ltd v Mitchell (1933)	52
Breen v A.E.U. (1971)	44
B.R.S. v A.V. Crutchley (1968)	245
Broome v Broome (1955)	76
Broome v Gosden (1845)	65
Buckoke v G.L.C. (1971)	56
Buckley v Tudge (V.O.) (1958)	190
Byrne v K.R.S. Ltd (1958)	44
Calcraft v Guest (1898)	77
Callis v Gunn (1964)	76
Calvert v Archbishop of Canterbury (1788)	74
Capital and Counties Bank v Henty (1882)	65
Cartwright v Sculcoates Union (1900)	188
Caton v Caton (1867)	74
Cescinsky v George Routledge & Sons (1961)	54
Chantrey Martin v Martin (1953)	71
Child v Affleck (1829)	59
Chubb v Flannagan (1834)	66
Coco v A.N. Clark (1969)	50

	Page
Conway v Rimmer (1968)	76, 79
Cramp & Sons v F. Smythson Ltd (1944)	43
Crompton Ltd v Commissioners of Customs and Excise (1972)	76
Day v Bream (1837)	63
Des Salles v Kensington & Chelsea LBC (1970)	192
Dodds v South Shields Assessment Committee (1895)	188
Duncan v Cammell, Laird (1942)	79
Durrell v Evans (1862)	75
Earl v Slater & Wheeler (1972)	45
Easton v Hitchcock (1912)	53
Edwards v S.O.G.A.T. (1970)	44
Emmens v Pottle (1885)	63
Evans v Harries (1856)	58
Evans v Hoare (1892)	75
Ex parte Campbell (1870)	77
Finlay v N.V. Kwik Hoo Tong (1929)	58
Fournet v Pearson (1897)	66
Fraser v Evans (1969)	54
Gartside v Outram (1856)	54
Gee v Pritchard (1818)	47
Ghani v Jones (1970)	76
Re Godden (1971)	44
Goodman v Eban (1954)	75
Grant v Knaresborough UDC (1928)	188
Grazebrook v Wallens (1973)	78
Groom v Crocker (1939)	58
Hall v Truman, Hanbury & Co. (1885)	72
Hankinson v Bilby (1847)	66
Harrison v Thornborough (1714)	65
Hawkins v Holmes (1721)	74
Hebditch v MacIlwaine (1894)	59
Helman v Horsham & Worthing Assessment Committee (1949)	193
Henley v Henley (1955)	78
Hennessy v Wright (1888)	80
Hickman v Maisey (1900)	43
In the goods of R.A. Usborne (1909)	75
Howard v Odhams Press (1938)	56

	Page
Hubbard v Vosper (1972)	55
Initial Services v Putterill (1967)	54
In re G (an infant) (1963)	123
J'Anson v Stuart (1787)	66
Jenkins v Gainsford & Thring	75
Jones v Great Central Railway (1910)	77
Kavanagh v Chief Constable of Devon & Cornwall (1973)	230
Kearsley v Philips (1883)	71
King v The Queen	76
Knüller v D.P.P. (1962)	46
Kuruma v The Queen	76
Ladbroke v William Hill (1964)	43
Laing v Kingswood Assessment Committee (1949)	191
Leggatt v Tollervey (1811)	76
Leslie v J. Young & Sons (1894)	43
Lewis v Daily Telegraph (1964)	66
Liquid Veneer Co. v Scott (1912)	49
Lloyd v Mostyn (1842)	77
Lobb & Knight v Stanley (1884)	74
London Assn for Protection of Trade v Greenlands (1916)	62
Longdon-Griffiths v Smith (1951)	59
Lyons v Wilkins (1899)	43
Mackenzie v Soden Mineral Spring Co (1891)	48
Magor & St. Mellons RDC v Newport (1952)	190
Malden & Coombe Corpn v Bennett (1963)	192
Martin v British Museum (1894)	63
Ministry of Housing & L.G. v Sharp (1970)	224
Mole v Mole (1950)	78
Morison v Moat (1851)	48
Morison v Turnour (1811)	74
Mortimer v M'Callan (1840)	72
Mourton v Hounslow LBC (1970)	192
Myers v D.P.P. (1964)	67
Newstead v London Express Newspapers (1940)	66
Microtherm Electrical Co v Percy (1957)	47, 49
Norwich Pharmacal v Commissioners of Customs & Excise (1973)	81
Nuttall v Nuttall & Twyman (1964)	78

	Page
Ogilvie v Foljambe (1817)	74
Osborn v Boulter (1930)	59
Pais v Pais (1970)	78
Pollard v Photographic Co (1888)	48
Pope v Curl (1741)	47
Prince Albert v Strange (1849)	47
Printers & Finishers Ltd v Holloway (1964)	49
Propert v Parker (1830)	74
Pullman v Hill (1891)	58
R v Architects Registration Tribunal (1945)	44
R v Bono (1913)	72
Reg v Cowper (1890)	75
R v Lewes Justices (1971)	80
Reg v Liverpool Corporation (1972)	230
Reg v L.C.C. ex parte Akkersdyk (1892)	230
Reg v Maqsud Ali (1966)	76
R v Mills (1962)	76
R v Payne (1963)	76
Reg v Stewart (1970)	76
Ratcliffe v Evans (1892)	58
Re D (1970)	124
Re J.S. (an infant) (1959)	123
Re M (1972)	123
Re P.A. (an infant) (1971)	123
Ridge v Baldwin (1963)	44
Robb v Green (1895)	47
Roberson v Rochester Folding Box (1902)	48
Robinson v Taylor (1948)	192
Rogers v Home Secretary (1972)	80
Saltman Engineering v Campbell (1948)	50
Saunders v Seyd & Kelly's Index (1896)	52, 235
Sayer v Glossop (1848)	72
Schneider v Norris (1814)	74
Seager v Copydex (1967)	50
Selby v Selby (1817)	74
Shaw v D.P.P. (1962)	46
Smith v East India Co. (1841)	80

	Page
Southwark L.B.C. v Williams (1971)	142
Stansbie v Troman (1948)	245
Stephenson, Jordan & Harrison v MacDonald & Evans (1952)	47, 50
Stokes v Moore (1786)	74
Stuart v Bell (1891)	59
Suhner v Transradio (1967)	50
Sun Life Assurance Co v W.H. Smith (1933)	64
Terrapin v Builders Supply Co (1967)	50
Toogood v Spyring (1843)	58
Vizetelly v Mudie's Library (1900)	63
Waterhouse v Barker (1924)	72
Watney Mann v Langley (1963)	189
Watson v Cammell Laird (1870)	77
Watt v Longsdon (1930)	58, 59
Weinberger v Inglis (1919)	44
Weld-Blundell v Stephens (1920)	237
Williams v Settle (1960)	43
Williams v Summerfield (1972)	72
Yovatt v Wingard (1820)	48

INDEX TO STATUTES

		Page
Adoption Act, 1958	s.40	122
Alkali, etc., Works Regulation Act, 1906	s.12	45
Children Act, 1948	s. 2	122
	s. 3	123
	s.14	121
Children & Young Persons Act, 1969	s. 2	120
	s. 9	122
	s.24	123
Chronically Sick & Disabled Persons Act, 1970	s. 1	122
Civil Evidence Act, 1968	s.5, s.10	68
Copyright Act, 1956	s. 2	43
Criminal Evidence Act, 1965	s. 1	68
Crown Proceedings Act, 1947	s.28	81
Education Act, 1944	s. 8	177
	s.48, s.81	178
Education Act, 1962	s. 2	178
Employment & Training Act, 1948	s.10, s.13	177
Furnished Lettings (Rent Allowances) Act, 1973		143
General Rate Act, 1967	s.108	187
	sched. 13	190
Housing Finance Act, 1972	sched. 3	143
	sched. 4	144
Local Authorities (Goods and Services) Act, 1970	s. 1	116
Local Authority Social Services Act, 1970	s. 2	121
Local Government Act, 1972	s.100, s.101,105,116	
Lord Cairns Act, 1858		47
Ministry of Social Security Act, 1966	s.16	193

		Page
National Assistance Act, 1948	s.21	142
Official Secrets Act, 1911	s. 2	45
Post Office Act, 1955	s.55	48
Post Office Act, 1969	s.65, s.80	45
Post Office (Data Processing) Act, 1967	s. 2	45
Public Bodies (Admission to Meetings) Act, 1960		105
Public Records Act, 1958	s. 5	45
Statute of Frauds, 1677	s. 4	73
Theft Act, 1968	s.13	46

INDEX TO SUBJECTS

	<u>Page</u>		<u>Page</u>
<u>ACCESS</u> control	91, 215	DHSS	125, 137, 145, 161, 193
Adoption	123		
Aggregation of data	103	<u>EDUCATION</u> Welfare	137, 178
Arrears	153, 187	Evidence	67, 228
Attitudes - public	29		
- social workers	139	<u>FRANKS</u> Committee	21, 238
Authentication	73, 90	Forms - contents	162, 179
		- "omnibus"	112
<u>BILLS</u> , Parliamentary	16, 17, 19 227, 231		
B.C.S.	221, 226	<u>GISP</u>	113
<u>CENTRALISATION</u>	201	<u>HOLDER</u> - definition	26
Chain model (data)	29, 56, 202, 243	- responsibilities	244
Child Guidance	179, 184	Housing - applications	147
Children in Care	122	- arrears	153, 160
Collector - definition	26	- transfers	152
- responsibilities	243	- visitors	149
Confidence	46		
Context-data	32, 112	<u>INDENTURE</u> - data	203
Copyright	43	Indid	25, 83
		Innuendo	65
<u>DATABANKS</u>	227	Inspection of files by public	221
Databank Board	225		
Databases	100	<u>LAMSAC</u>	113, 146
Data-dependent checks	93, 94, 97	Local authorities	
Defamation	56	- computer consortia	115
Devolved access control	201	- reorganisation	104
		- responsibilities	239

	<u>Page</u>		<u>Page</u>
LOLA	24, 110	<u>SATELLITE</u> installations	204
		Scandinavia	9, 186, 219
<u>MEDICAL</u> records	137, 182	Schools	176
		Security	83
<u>NATURAL</u> justice	44, 123	Shared systems	115
Negligence	35, 64, 237	Surveillance Systems	7, 11, 89
NHS	138		
		<u>TERMINALS</u>	86
<u>OMBUDSMAN</u>	105, 240	Theft	46
		Trespass	43
<u>PASSWORDS</u>	90		
Planning	217	<u>USER</u> - definition	26
Post Office	45	- responsibilities	245
Print-outs	219	- identification	87
Privacy	10, 141, 185, 196, 248	USA	17, 109, 182, 219
Privilege - defamation	58		
- evidence	76	<u>VALUATION</u> , rating	188
- in systems	97		
Privtype	206, 245	<u>YOUTH</u> Employment	177, 180
Professions	246	Younger Committee	21, 42, 220 223, 228
Public Interest, the	54		
<u>RACE</u>	11, 146, 155		
Rebates - rents	137, 143, 154		
- rates	137, 193		
Religion	11, 123		