ISSN 0254-2757

QI QUAESTIONES INFORMATICAE

Volume 4 Number 3

October 1986

J. Mende	**Laws and Techniques of Information Systems**	**1**
S. Berman and L. Walker	**A High-Level Interface to a Relational Database System**	**7**
K.G. van der Poel and I.R. Bryson	**Protection of Computerised Private Information: A Comparative Analysis**	**13**
P.J.S. Bruwer and J.M. Hattingh	**Models to Evaluate the State of Computer Facilities at South African Universities**	**21**
P. Machanick	**Low-Cost Artificial Intelligence Research Tools**	**27**
S.P. Byron-Moore	**What's Wrong with CP/M?**	**33**
R.F. Ridler	**In Praise of Solid State Discs**	**39**
C.W. Carey, C. Hattingh, D.G. Kourie, R.J. van den Heever and R.F. Verkroost	**The Development of an RJE/X.25 Pad: A Case Study**	**45**
D.G. Kourie	**A Partial RJE Pad Specification to Illustrate LOTOS**	**59**
	BOOK REVIEWS	**6, 20**

An official publication of the Computer Society of South Africa and of the South African Institute of Computer Scientists

'n Amptelike tydskrif van die Rekenaarvereniging van Suid-Africa en van die Suid-Afrikaanse Instituut van Rekenaarwetenskaplikes

QUÆSTIONES INFORMATICÆ

An official publication of the Computer Society of South Africa and of the South African Institute of Computer Scientists

'n Amptelike tydskrif van die Rekenaarvereniging van Suid-Africa en van die Suid-Afrikaanse Instituut van Rekenaarwetenskaplikes

Subscriptions

Annual subscriptions are as follows:

	SA	US	UK
Individuals	R10	$ 7	£ 5
Institutions	R15	$14	£10

Circulation and Production

Mr C.S.M. Mueller
Department of Computer Science
University of the Witwatersrand
1 Jan Smuts Avenue
Johannesburg, 2001

Quæstiones Informaticæ is prepared by the Computer Science Department of the University of the Witwatersrand and printed by Printed Matter, for the Computer Society of South Africa and the South African Institute of Computer Scientists.

PROTECTION OF COMPUTERISED PRIVATE INFORMATION: A COMPARATIVE ANALYSIS

K.G. van der Poel
Department of Medical Informatics
Groote Schuur Hospital
Observatory 7925

I.R. Bryson
Graduate School of Business
University of Cape Town
Rondebosch 7700

The principles of protection of private information have gradually been defined during the last decades. The US Privacy Act of 1974 regulates practices of the federal government. Two committees of the UK government have prepared the Data Protection Act of 1984. Codes of practice play an important role in the Netherlands. In South Africa, data privacy is protected by the law of delict. However this provides a weak and reactive opportunity for redress. While the law commission is preparing to study the subject in depth, professional organizations should establish codes of practice.

1. INTRODUCTION

George Orwell foresaw a rather unpleasant society in 1984. In that society every aspect of human life was centrally controlled by a power that had access to and could manipulate information about all citizens at all time. Individual privacy and the right of a person to restrict and control information about himself were totally denied.

The year 1984 has passed. Orwell's predictions have not materialized, or at least not quite. The possibility that personal privacy could be eroded by unbridled use of technology has, however, been a concern to many people. Steps have therefore been taken to redress the balance and legislation has been passed in several countries. In the following, an overview is given of some of these measures and the principles on which they are based and conclusions are drawn for South Africa.

2. PRIVACY

Privacy is easy to understand, but hard to define precisely. McQuoid-Mason[1] quotes the following descriptive definition by Westin:

> "The essence of privacy is no more and certainly no less, than the freedom of the individual to pick and choose for himself the time and circumstances under which, and most importantly, the extent to which, his attitudes, beliefs, behaviour and opinions are to be shared with or withheld from others. The right to privacy is therefore a positive claim to a status of personnel dignity - a claim for freedom, if you will, but freedom of a very special kind."

The general concept of privacy as a civil right is well anchored in Western civilization. Safeguards against the invasion of privacy are found in Roman Law, Jewish Law and English Law. Concepts such as dignity, honour and human rights are closely related to it. John Locke wrote: "Everyman has a property in his own person. This nobody has a right to but himself." Judge Cooley defined it as "the right to be left alone". John Stuart Mills said: " There is a limit to the legitimate interference of a collective opinion with individual independence and to find that limit ... is indispensable to a good condition of human affairs".

Invasions or violations of privacy under modern legislation are divided into 4 categories: intrusions of the private sphere, public disclosure of private facts, placing a person in false light, and appropriation of another's name or likeness.

The second and third of these invasions of privacy have very much to do with practices of data collection, storage and dissemination. The defence against them is called data privacy. As technological development influences the need and the capacity for data privacy, it is to be expected that legislation must be continuously adjusted to make sure the balance of right and wrong is not upset. It may be worth emphasizing that concern for data privacy does not imply the intention to protect people who have something to hide such as crimes or trespasses or tax evasion. Its intention is to ensure that a proper balance is struck between the interests of the individual and those of the community or, for that matter, of the dominant groups in the community.

3. COMPUTERS AND PRIVATE INFORMATION

Private information is loosely defined as all information concerning an individual. It includes information which is generally considered to be in public domain, such as name and address. It also includes information which is more sensitive or confidential, such as data about diseases, religion, possessions and debts, tastes and preferences etc. The advent of computers has had a significant effect on the ability to collect, store and disseminate private information in such a way that data privacy may be affected.

Computers have had several negative effects on data privacy: firstly private information is no longer confined to the place and format in which it was collected. It can now be be transmitted, collected and retrieved with very little effort. Secondly private information has become much more accessible and access to the data may be totally unobserved. Thirdly, data may be corrupted without any indication that this has happened.

The use of computers can also have positive effects on data privacy. Proper controls make it possible to limit access to private information effectively. Advanced processing techniques make inspection and correction feasible. Appropriate security measures make corruption virtually impossible.

The conclusion is that computer technology is capable of either undermining or supporting data privacy in a big way. In the following, some examples will be considered of how different countries have dealt with this problem.

4. MOVES TOWARDS LEGISLATION

The desire to formally protect data privacy can be traced to an article by Warren and Brandeis in 1890.[2] For the first time they presented arguments to establish an explicit legal defence against eavesdropping, illegal search and seizure or publication of private facts. This was followed by the City of New York enacting the first modern statute to protect data privacy in 1902.

With the advent of computers, a number of countries reacted by drafting specific legislation to protect data privacy. A list of the nations that took such action before 1984 is shown in Table 1. It is interesting to note that this list closely resembles the list of the more developed nations.

The first specific legal protection of computerised data was through the enactment of the Land of Hessen Data Protection Act of 1970. This act applied to private information held by local and public bodies within the jurisdiction of this German province (Land). The purpose of the act was to:

> "lay down penalties for the examination, alteration, extraction and destruction of data by unauthorized persons, and provide for the correction of inaccurate data and for the appointment of a data protection commissioner to oversee the handling of information provided by individuals and the consideration of complaints."[3]

The first national act was the Swedish Data Act of 1973. This is hardly surprising as Sweden has a long history of legislature which gives citizens access to any information assembled by the state.

The Swedish Data Act was followed by the American Privacy Act of 1974 and subsequently by many other national data protection acts. These regulations vary greatly in extent and nature. For example Canada regulates only the government and the public activities, while most other nations regulate both the public and private sector data processing societies. Denmark even has separate acts for private and public data holders. Common to all, though , are regulations governing the right of access by an individual to his records and certain controls on the establishment and operation of databases for private information. The regulations generally apply to all personal information with specific exemptions in respect of national security, the administration of justice and other critical activities e.g. health care. In some cases insignificant little data bases are exempted. In other cases certain types of sensitive data (e.g. religion, political affiliation) are subject to extra controls.

In 1984 the Data Privacy Act was promulgated in the United Kingdom. This was the result of extensive deliberations of 2 committees and will be reviewed below.

Legislation has been under consideration in the Netherlands for the last 10 years. The situation in this country will all be reviewed below.

Australia	P	L	R
Austria		L	
Belgium	P		R
Brazil	P		
Canada		L	R
Columbia	P		
Denmark		L	
Finland	P		R
France		L	
Germany	P	L	R
Greece			R
Hungary		L	
Iceland		L	
Ireland			R
Israel		L	
Italy	P		R
Japan			R
Luxembourg		L	
Netherlands	P		
New Zealand		L	
Norway		L	R
Portugal	P		
Spain	P		
Sweden		L	R
Switzerland	P	L	R
Turkey			R
UK		L	R
USA	P	L	R
Yugosalvia			R

Key: L = law adopted P = legislation proposed R = government report

Source: Transnational Data and Communication Report January 1986

table 1
Status of data protection legislation - 1986

5. THE UNITED STATES PRIVACY ACT OF 1974

There has been a groundswell of support for limitations to the secrecy of government information in the United States. Increasing use of secretive operations and classification of papers after the second world war drew sharp criticism. “If government is to be truly of, by and for the people, the people must know in detail the activities of government.”[4]

This movement led to the promulgation of the Freedom of Information Act in 1966. This gave all persons the judicially enforcable right to see the records of federal government agencies, except to the extent that the records may be covered by an exemption. However, it was soon found that this act was far from ideal as government agencies were only obliged to show final documents, not the supporting details and could charge exorbitant fees for the search effort.

Against this background, the Privacy Act of 1974 was enacted. The purpose of the act was clearly stated in its preamble: "To safeguard individual privacy from the misuse of the federal records and to provide that individuals be granted access to records concerning them which are maintained by federal agencies."[5]

The act was deliberately restricted to federal agencies because of the complexity of the statute that would have been required if private agencies were similarly regulated.

Some of the salient provisions of the law follow.

- The retention of personal data is limited: "each agency shall maintain in its records only such information about an individual as is relevant and necessary to accomplish the purpose of the agency".
- Procedures for the collection of data prescribed: "agencies should collect information to the greatest extent practicable directly from the individual".
- The right of notification required the agency to publish in the Federal Register the existence and character of the system of records - including name and location of the system and nature of the files maintained.
- The right of access of the subject is arranged: "Each agency shall upon request by any individual ... permit him to review the record and have a copy made of all or any portion thereof in a form comprehensible to him."
- Concern for the accuracy of data is required: "an agency shall maintain all records about an individual with such accuracy, relevance, timeliness and completeness as is reasonably necessary to assure fairness to the individual".

Regulations governing the dissemination to other agencies and non-government users are comprehensively specified in the act. In most cases the subject must give written permission before the record can be disclosed to other users, while agencies must keep accurate accounts of the nature and purpose of a disclosure.

The act specifies that non-observance may lead to both civil and criminal charges. It does not go as far as establishing a special data protection authority.

Discussion

The act has been in force for over 10 years. Its main benefit appears to be that it has served as a standard of good data processing practice. A commission charged with recommending to congress any changes to the act reported in 1977. Its recommendations included the establishment of a data privacy board and many technical corrections. They did not recommend extension of act's coverage to the private sector.[6] In fact, the act has not been altered significantly since these recommendations.

6. THE UK DATA PROTECTION ACT OF 1984

The Data Protection Act is a result of over twelve years of parliamentary effort, based on the work of two major committees of enquiry. These were the Committee on Privacy (Younger Committee) reporting in 1972 and the Data Protection Committee (Lindop Committee) reporting in 1978.

The Younger Committee examined the entire subject of personal privacy. It considered "the computer problem as it affects privacy in Great Britain to be one of apprehensions and fears and not so far one of fact and figures". As a result, the committee wanted to keep the dangers of privacy arising from computers in perspective and did not propose any specific legislation. However, the committee did formulate some important principles for the proper handling of private information. These are known as the Younger Committee principles. They are shown in table 2.

1. Information should be regarded as held for a specific purpose and should not be used, without appropriate authorization, for others.
2. Access to information should be confined to those authorized to have it for the purpose for which it was supplied.
3. The amount of information collected and held should be the minimum necessary for the achievement of the specified purpose.
4. In computerised systems handling information for statistical purposes, adequate provision should be made in their design and programs for separating the identities from the rest of the data.
5. There should be arrangements whereby the subject could be told about the information concerning him.
6. The level of security to be achieved by a system should be specified in advance by the user and should include precautions against the deliberate abuse or misuse of information.
7. A monitoring system should be provided to facilitate the detection of any violation of the security system
8. In the design of information systems, periods should be specified beyond which information should not be retained.
9. Data held should be accurate. There should be machinery for the correction of inaccuracy and he updating of information.
10. Care should be taken in coding value judgements.

table 2

The Younger Committee principles for handling personal information by computer [7]

The Lindop Committee was established in 1975, as a result of a recommendation of the Younger Committee, to advise the government about legislation to protect personal data handled in computerised systems. The committee recommended seven principles as the basis for legislation. (see table 3). It further recommended the institution of a Data Protection Authority, establishment of codes of practice and enactment of a law control computerised private information. These recommendations led to the Data Protection Act of 1984.

1. Data subjects should know what personal data is held, why and how it will be used, by whom and for what purpose, and for how long.
2. Personal data should only be used for purposes made known when it is collected.
3. Personal data should be accurate, complete, relevant and timely.
4. The minimum amount of data should be used.
5. Data subjects should be able to verify compliance.
6. Users of data should be able to do so for their lawful interests without undue costs or use of their resources.
7. The community at large should enjoy any benefits and be protected from any predjudice, which may flow from the handling of personal data.

table 3

The Lindop Committee principles for data protection legislation

The purpose of the Data Protecton Act is: “to regulate the use of automatically processed information relating to individuals and the provision of services in respect of such information”.[8]

The office of a Data Protection Registrar is created, whose duty it is to promote the observance of the data protection principles by data users and persons carrying on computer bureaux.

To be legal, all personal data files must be registered with the office of the Registrar, giving particulars about purpose and content of the file.

The Act stipulates that personal data shall be obtained fairly and lawfully and that the purpose for which data is collected should be clear to the data subject.

Codes of practice, although recommended by the Lindop committee, are not prescribed in the law, but it is left to the registrar to encourage such arrangements.

The right of access of data subjects is guaranteed, in that individuals are entitled: "to be informed by any data user whether the data held by him include personal data of which that individual is the subject, and to be supplied by any data user with a copy of the information constituting any such personal data held by him". The data user may request a fee for such access, up to a prescribed maximum.

Although the subject can challenge the accuracy of the record, he is limited in his ability to force the data user to amend the record or to claim damages for the inaccuracy.

The Act contains virtually no regulations concerning the dissemination of data. As a consequence, unhindered transfer of data between registered users may occur, provided both parties are registered and legitimate users of such data.

Discussion

In accordance with the title of the Act, great emphasis has been placed on the control of information (protection) rather than the type of information (privacy). A positive aspect of the Act is certainly the fact that both the government and private systems are covered. A major problem is that it applies to all computerised files, regardless of the number of records or their content. This is likely to lead to considerable expense for the large number of small users. An aspect which is often queried is the omission of codes of practice. These could have been used to regulate certain types of files more precisely.

7. PROPOSED LEGISLATION IN THE NETHERLANDS

The move towards specific legislation to protect data privacy started in the Netherlands in 1972. One of the reasons was the popular resistance to the census of 1971. The move resulted in an elaborate proposal of law, 23 pages long, introduced in 1981. After long deliberation this proposal was withdrawn and replaced by a simpler proposal, consisting of 12 pages.[9] The present proposal is still far reaching in that it covers computerised as well as manual, and governmental as well as private files containing personal information. It requires registration of all such files and contains the normal safeguards of protection against unauthorized use and access by the data subject.

An interesting feature of the proposal is that special provision is made for codes of practice and privacy regulations to be promulgated by specific sectors. Voluntary regulations have, in fact already been in force in several sectors such as municipalities, health care, etc. The understanding is that the new law will mainly serve as a framework for these regulations.[10]

8. INTERNATIONAL REGULATIONS

Several international agencies have involved themselves with aspects of the protection of information. The purpose was to promote the rights of the individual in the member states and to avoid unfair competition. Such unfair competition could occur if member states adopted widely different practices, but also if the rights of the member state citizens could be circumvented by transferring data abroad to "countries of convenience".

In 1980 the Organization for Economic Cooperation and Development (OECD) issued "guidelines governing the protection of privacy and transborder flows of personal data" thus standardizing to some extent the principles of personal information handling in its 24 member states. An important stipulation is the provision that the transfer of personal data to countries not observing adequate privacy protection may be limited. The guidelines of the OECD are, however, not binding to member states.

The Council of Europe accepted a convention of rules concerning automated processing of private information in 1981. These rules follow the stipulations of the OECD very closely. They are expected to become binding on the member states in 1986.[11]

9. LEGAL PROTECTION IN SOUTH AFRICA

There is presently no specific law in South Africa concerning private information. For the protection of data privacy, the individual must therefore rely on the general principles of Roman Dutch law. The basis for any action lies in the law of delict. The law of delict provides for compensation for unlawfully inflicted injury to a person.[12] Invasions of data privacy can conceivably be actioned under the Actio Injuriarum or the Law of Defamation.

The Actio Injuriarum redresses wrongs to interests of personality generally. Its scope has been described: "to embrace all willful invasions of rights of another, which every man has as a matter of natural right in respect of his person, his dignity and his reputation".[13] However, it is generally considered that the stringent requirements of this Actio are unlikely to be met by a data privacy case.

The Law of Defamation protects the reputation. The delict of defamation is described as: " the unlawful publication animo injuriandi (with intent to injure) of a statement concerning another person which has the effect of injuring that person in his reputation".[15] There are various defences against this action, notably those of justification, qualified privilege and willing consent. These defences make it unlikely that this action will be applicable except in the most blatant situations.

It would therefore appear that the currently available protection of data privacy in South Africa is very limited. An action would only be successful after gross abuse. It is also a reactive form of redress. The specific legislation adopted in other countries has the merit that it is largely pro-active i.e. enforces and controls certain standards of behaviour.

10. THE ROAD AHEAD

There appears to be a disparity between the protection of data privacy under existing South African law and under the new legislation and rules adopted in most developed countries. There is no obvious reason for this disparity to persist: the sophistication of private information handling is at least at a par and the people are no less keen on their civil liberties. Already, the SA law commission has recognised the discrepancy and has identified the area of data privacy as requiring investigation as part of project 44: "A comprehensive and comparative enquiry into the protection of all rights of personality". However, other pressing needs for legislation may keep this project from being undertaken for some time.

The remaining option is that interested groups and parties get together in the short term to consider voluntary codes and regulations. Such regulations could set standards for responsible data processing behaviour. If these regulations would be adopted by professional societies such as the Computer Society, the Medical and Dental Association and the Institute of Chartered Accountants, then meaningful protection would be provided in the vast majority of situations. General acceptance of such regulations might even forestall the need for legislation. At present a draft code of conduct is being studied by the Computer Society of South Africa. Adoption, promulgation and further discussion of this code will set an example, likely to be followed by others.

REFERENCES

1. McQuoid-Mason, DJ (1978). *The law of privacy in South Africa..*, Juta & Co. Cape Town.
2. Warren, S and Brandeis, L (1890). The right to privacy. *Harward Law Review* , 4 p 193.
3. Home Secretary (1975). *Computers and Privacy.* HMSO. London p 313.
4. Michigan Law Review (1975). Government information and the rights of citizens. *Michigan Law Review,* May-Jun 1975.
5. U S Congress (1974). Privacy Act 1974. Washington. *United States Government code 5 Section 552 (a).*
6. American Enterprise Institute (1979). *Privacy Protection Proposals.* Washington.
7. Younger, K (1972). *Report of the committee on privacy.* HMSO. London.

8. Data Protection Act (1984). HMSO. London.
9. Minister van Justitie (1982). *Wet persoonsregistraties.* Staatsdrukkerij Den Haag.
10. Holvast J (1986). Wet persoons registraties. *Informatie* **28** , May 1986.
11. Kuitenbrouwer, F (1984). *Privacy en persoonsregistratie: een overzicht..* Kluwer. Deventer.
12. Boberg PQR (1984). *Law of delict.* Juta & Co. Cape Town.
13. De Villiers JA (1922). Case: Matthews v Young AD 492.
14. Price E (1986). No place to hide. *Financial Mail* 28 March 1986 p 93.
15. Kinghorn, C (1979) *Defamation law of South Africa* , 7. Butterworth & Co. Cape Town.
16. McQuoid-Mason, DJ (1978). *The law of privacy in South Africa.* Juta & Co. Cape Town p198.

BOOK REVIEW

An Introduction to LISP, A. Narayanan and N. E. Sharkey, Ellis Horwood, 1985. ISBN 0–85312–968–1. 227 pages.

Reviewed by: Philip Machanick, *University of the Witwatersrand, Johannesburg 2001*

The growth of Artificial Intelligence and the proliferation of low-cost implementations of AI languages has created a demand for books offering a less formal treatment than that of established text books. Such books need to present carefully chosen subsets of a complex language—and a complex application area. Furthermore, they need to explain difficult concepts to the uninitiated in a comprehensible way.

Narayanan and Sharkey have succeeded in some respects in meeting these needs. Their choice of examples—based largely on describing parts of robots—has more appeal than the all-too-common approach of introducing arbitrary names for variables and functions—such as FOO and BAR. Furthermore, they have not shied away from introducing recursion before other forms of iteration, nor from using an almost purely functional style in the opening chapters. The sections on semantic nets and the blocks world are ambitious for a beginner's text and well executed, if a bit brief for the intended readership.

However, the book is marred by flaws in the authors' understanding of several key concepts. Examples include the stack mechanism, lexical scoping and reader macros. While most of these problem areas will not impact the beginner's conceptual grasp of LISP programming, they are a disappointment. An anomoly for a non-technical treatment is the amount of space devoted to describing the cons-cell representation of lists. Of more concern is the lack of consistency in the choice of dialects for examples. DEFUN is mostly used to define functions, while DF and DM are introduced to define FEXPRS and MACROS. A substantial example towards the end of the book is clearly not in the same dialect as the other examples.

Perhaps if Common LISP does become a widely accepted standard (even on "small machines"—some of which at least have enough memory), the difficulties relating to dialects will be overcome. At least appendices giving details of several dialects are provided.

Despite some well-executed diagrams, the casual reader is more likely to be put off by mediocre typesetting than by innaccuracies of detail. A further negative point is the over-use of "cute" names (Ann Droid the robot) and subheadings (The Pros of CONDs). But perhaps the sentence on page 141 makes it all worthwhile:

> Artificial Intelligence is the study of metal faculties …

NOTES FOR CONTRIBUTORS

The purpose of the journal will be to publish original papers in any field of computing. Papers submitted may be research articles, review artilces and exploratory articles of general interest to readers of the journal. The preferred languages of the journal will be the congress languages of IFIP although papers in other languages will not be precluded.

Manuscripts should be submitted in triplicate to:

Prof. G. Wiechers
INFOPLAN
Private Bag 3002
Monument Park 0106
South Africa

Form of manuscript

Manuscripts should be in double-space typing on one side only of sheets of A4 size with wide margins. Manuscripts produced using the Apple Macintosh will be welcomed. Authors should write concisely.

The first page should include the article title (which should be brief), the author's name and affiliation and address. Each paper must be accompanied by an abstract less than 200 words which will be printed at the beginning of the paper, together with an appropriate key word list and a list of relevant Computing Review categories.

Tables and figures

Tables and figures should not be included in the text, although tables and figures should be referred to in the printed text. Tables should be typed on separate sheets and should be numbered consecutively and titled.

Figures should also be supplied on separate sheets, and each should be clearly identified on the back in pencil and the authors name and figure number. Original line drawings (not photocopies) should be submitted and should include all the relevant details. Drawings etc., should be submitted and should include all relevant details. Photographs as illustrations should be avoided if possible. If this cannot be avoided, glossy bromide prints are required.

Symbols

Mathematical and other symbols may be either handwritten or typewritten. Greek letters and unusual symbols should be identified in the margin. Distinction should be made between capital and lower case letters; between the letter O and zero; between the letter I, the number one and prime; between K and kappa.

References

References should be listed at the end of the manuscript in alphabetic order of the author's name, and cited in the text in square brackets. Journal references should be arranged thus:

1. Ashcroft E. and Manna Z., The Translation of 'GOTO' Programs to 'WHILE' programs., *Proceedings of IFIP Congress 71*, North-Holland, Amsterdam, 250-255, 1972.
2. Bohm C. and Jacopini G., Flow Diagrams, Turing Machines and Languages with only Two Formation Rules., *Comm. ACM,* **9**, 366-371, 1966.
3. Ginsburg S., Mathematical Theory of Context-free Languages, McGraw Hill, NewYork, 1966.

Proofs and reprints

Proofs will be sent to the author to ensure that the papers have been correctly typeset and *not* for the addition of new material or major amendment to the texts. Excessive alterations may be disallowed. Corrected proofs must be returned to the production manager within three days to minimize the risk of the author's contribution having to be held over to a later issue.

Only orginal papers will be accepted, and copyright in published papers will be vested in the publisher.

Letters

A section of "Letters to the Editor" (each limited to about 500 words) will provide a forum for discussion of recent problems.