THE SALZBURG SEMINAR

TELECOMMUNICATIONS: POLICY ISSUES & REGULATORY PRACTICES AFFECTING THE FUTURE

SESSION 243, 29 June - 4 July 1985

REPORT ON GROUP D - SOCIAL & LEGAL ISSUES

THE SALZBURG SEMINAR

TELECOMMUNICATIONS: POLICY ISSUES & REGULATORY PRACTICES AFFECTING THE FUTURE

SESSION 243 - 29 JUNE - 6 JULY, 1985

REPORT ON GROUP D - SOCIAL & LEGAL ISSUES

PARTICIPANTS

1. The following were the participants in Group D:-

Faculty: The Hon. Justice Michael Kirby, CMG
President, Court of Appeal, Sydney, Australia
Chairman, OECD Expert Group on TDF & Privacy. 1978-1980.

Fellows:	Asher Arian	(Israel)
	Michael Buckley	(USA)
	Susan Kirk	(USA)
	Jorma Kuopus	(Finland)
	Ian Lloyd	(UK)
	Paraskevi Perrakis	(Greece)
	Leonarda Reut-Sadoswka	(Poland)
	Michael Ryan	(Canada)
	Luigi Di Paola	(Italy)
	Srecko Seljan	(Yugoslavia)
	Shahinaz Talaat	(Egypt)
	Bent Thorndahl	(Denmark)
	Oya Tokgoz	(Turkey)

and other Fellows who visited Group D.

Participants:

Ambassador L.H. Marks	(Chairman #243)
Mr. H.P.Gassmann	(OECD Secretariat)

BASIC TEXTS

2. The basic texts for the study of the Group were:

A.F. Westin	- How can we Protect Privacy in the Highly Advanced Information Society? unpublished paper for 1985 N.I.T. symposium, Japan.
M.D. Kirby	- The Morning Star of Information Law and the need for a greater sense of Urgency - Paper for the IBI Second World Congress on TDF, Rome 1984. See Summary 1984/3 Agora 31 (IBI)
OECD	- Guidelines on Transborder Data Barriers and the Protection of Privacy, 1980, Paris.
	- Transborder Data Flows - Proceedings of an OECD Conference, London 1983 North-Holland, Ch VII.
G.T. Marx	- "I'll be Watching You" in Dissent, Winter 1985, 26.

GENERAL THEME

3. The general theme of the group was consideration of the social, legal, cultural and political impact of TDF on individual countries, the global community and its institutions. A subsidiary and related theme was the

institutional arrangements that would be necessary to address the many issues presented by informatics generally and TDF in particular.

PARTICULAR TOPICS

4. The participants in Group D met on four occasions. At the first, the group, in discussion with Justice Kirby, decided on the structure of the seminars. It was decided to address the following issues in turn:-

1. Privacy protection.
2. Freedom of information.
3. Computer Crime.
4. Vulnerability of the Wired Society.
5. Sovereignty & Cultural Integrity.
6. Intellectual Property and Business Law.
7. Information Security.
8. Institutional Considerations.
9. Conclusions: Optimism or Pessimism?

PRIVACY PROTECTION

5. The session on Privacy protection opened with an explanation and description by Justice Kirby of the way in which informatics and TDF had been seen as causing dangers to privacy of individuals. the great growth in the capacity to collect personal data, the ever diminishing cost, the speed of retrieval, the permanency of availability and the absence of established legal protections all demanded responses by municipal regimes to the social problems then perceived to be created. This demand was voiced against the background of the moves following the Second World War to express human

rights in international instruments. Reference was made to the provisions on the right to information (and the countervailing rights to privacy) in the provisions of the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and then the series of international instruments addressed to the specific issue of data protection (privacy). These were the Nordic Council Resolution, the Resolutions of the Council of Europe, the Resolutions of the European Parliament and the Council of Europe Convention. The last mentioned, having just secured the fifth signatory will come into force in October, 1985. Meanwhile the OECD in 1985 agreed on Guidelines on Privacy which had been accepted by all OECD countries except Ireland. These Guidelines were proving influential in the design of local laws on privacy or data protection in a number of countries.

6. The international, instantaneous nature of TDF made international solutions to privacy necessary. A novel problem was presented. By keeping data in data bases outside a jurisdiction, but retrievable in that jurisdiction, the effective control of a country over such data would be lost or severely diminished. Hence the demand for international action for two reasons - both related to transborder data flows (TDF).

* The ineffectiveness of municipal law, unaided by international cooperation to preserve privacy.

* The inefficiency, in such a medium, of

adopting radically different principles which would be expected to operate simultaneously in the same data, accessible in numerous countries.

The realisation of these problems has provided a new and powerful impetus to international cooperation in rules for the social fall-out of informatics. In the developed world the focus has been OECD and the Council of Europe. The interests of the developing countries have tended to be considered by the Intergovernmental Bureau for Informatics (IBI) and, belatedly, UNESCO.

7. The group considered the OECD Guidelines. The basic principles can be summarised (as related to the throughput of data in an information system) as follows:-

- Personal data should be collected, stored and communicated only for specified and legitimate purposes with the authority of the data subject or authority of law.
- Personal data for the uses to which it is to be put should be accurate, up to date, relevant and not excessive.
- The data subject should be entitled upon request, to be informed by a data controller whether he holds data relating to him and to have access to that data - with exceptions spelt out by law.

8. Discussion of these privacy concerns in the Group centred on such matters as:-

* The relative effectiveness of courts, Ombudsmen and other means to provide accessible, cheap and trustworthy protections for the citizen concerned about misuse of personal data.
* The ability of judges and bureaucrats to understand the new media in order to be able to provide effective protection to citizens affected by it.
* The limits, if any, in the access to data banks by police and other authorities faced by serious crime. The difficulty of drawing a line to limit such access in cases of suspected terrorism and breaches of national security.
* The new challenges to professional confidentiality by the effective access to a large variety of medical data in computerised form.
* The issue of whether individual privacy was a real concern of newly industrialised countries and developing countries generally - or whether it was just a middle class anxiety of developed countries.
* The differing traditions and concerns - even in developed countries, such as Japan.

9. Justice Kirby outlined a number of the debates which had surrounded the design of privacy laws. He mentioned

* The issue of omnibus legislation v piecemeal

laws: ie whether it was preferable to address issues such as banking privacy separately or as part of a general conceptual law on privacy (data) protection.

* The issue of automated data: whether laws should concentrate on informatics only or on personal data, whether automated or in manual files.

* The legal person issue: whether privacy rights should extend to legal persons or be restricted, as an aspect of human rights, to natural persons only.

* The institutional issue: whether courts or ombudsmen or other means (licensing tribunals, Human Rights Commissions) should be used for effective privacy/data protection. It was generally considered that each country would have to develop its own remedies. The achievement of simple, easily understood general principles of "fair information practices" would be a contribution to harmonisation of laws. Endeavouring to harmonise institutional arrangements was bound to fail and was in any case unnecessary to achieve effective data protection in TDF.

10. The group debated, however, the suggested deficiencies of licensing of data banks - given the vast increase in the use of personal computers. The need to avoid laws which are technology specific was also stressed.

FREEDOM OF INFORMATION

11. The Group considered the implications for TDF of freedom of information laws. The link between such laws and the central provision of privacy/data protection laws was observed, namely access to data. The Group was informed of the case mentioned by J. Bing of a Norwegian social scientist who accessed a terminal in Washington DC under the United States FOI to secure NATO deployments in Norway. However, this was a State secret in Norway. The ineffectiveness of municipal secrecy laws, once FOI permits access in some jurisdiction, was seen as yet another example of the breakdown of municipal sovereignty by the force of TDF. In many ways this would be a good thing. Information technology generally challenges secrecy and closed bureaucratic habits. The photocopier was already a powerful weapon for greater openness. However, TDF would also contribute to the haemorrhaging of information considered secret or confidential by some holders of it.

12. Some countries such as the United Kingdom, were resisting the enhancement of legal rights of access by citizens to government information in right of citizenship and to make democracy. Other countries (such as Australia, Canada and New Zealand) had, on the other hand, recently enacted FOI laws. In Europe, the Committee of Ministers of the Council of Europeis reviewing Article 10 of the European Human Rights Convention to see if Article 10 can be enhanced to increase FOI rights in those countries which do not have

them in municipal law. However in the USA, Australia and other countries there has lately been a backlash based partly on considerations of costs and partly because of a feeling that FOI is being used more by business to get information that will help it to outmanoeuvre government - rather than citizens enforcing democratic rights. This concern will need to be addressed - as will the impact of information technology on FOI. The possible use of informatics to enhance democratic opinion sampling was discussed by the Group.

COMPUTER CRIME

13. Justice Kirby pointed to some of the problems which had emerged in respect of computer crime - informatics and TDF. He said the problems could be considered on two levels.

The first was the need to adapt current laws practices, institutions and law enforcement to cope with anti-social manipulation of iinformation technology. He referred to the need to redefine "theft" which, in comme law countries traditionally implied carrying away "goods". In information crime, no goods may be taken - simply information which had a value divorced from a physical object. He also referred to the need to change police recruitment, rules of admissible evidence in criminal trials and training of lawyers and judges to cope with information technology. He also said that new international law would

be needed to cope with transborder crimes - ie a terminal might be accessed in Country A, the message may be received in countries B, C and D and transmitted to do damage in countries X, Y and Z. Whose law would apply? Whose police would investigate? Whose courts would have jurisdiction to try? Whose prisons would receive the info-criminal? Mention was also made of difficulties of detection. The value of code words and encryption was stressed; but these may be of limited use against an "inside job" by a trusted member of the computer staff with full access to the data.

A second level is the impact on social peacefulness and lawful abiding conduct caused by dislocation and unemployment. If large numbers - especially of young persons - are out of work for long periods because of the impact of informatics on societies, what consequence will this have upon peace, law and order and traditional civil liberties?

VULNERABILITY

14. Considerable time in the Group was spent discussing aspects of the vulnerability of the informatics society. Justice Kirby outlined the results of a Swedish study published under the report Vulnerability of the Wired Society. This report suggested the need for administrative and even legal measures to protect society as a whole and groups in society from

unacceptable damage by destruction of data of vital importance, held upon a few tapes liable to loss or destruction by:

- operator error
- accidents
- natural disasters
- terrorist acts
- industrial disruption
- espionage - national or business

This problem also has an international dimension. Vital data kept in one country - and accessed in another by TDF might suddenly become unavailable because of political or economic events.

15. The Group discussed the possibility of backup copies - something the Swedish report had recommended for truly vital national data. However, it was suggested that some risk taking was inevitable - involving a weighing of the risk and the acceptability of loss or damage. A cost/benefit equation had to be done in each case. But it was important that the risks be considered.

SOVEREIGNTY, CULTURE, ALIENATION

16. The Group then turned to the impact of new information technology on national sovereignty and culture and individual alienation. The overwhelming influence of Anglophone systems in mass media and other information flows was seen as a threat to more vulnerable languages and cultures in some countries. Reference was made to cheap saturation of the media by cheap reruns of North American "soap operas". The fear has been expressed by

one French Minister that the future history of France may be written from English language translations of Le Monde kept in a Chicago data base. Justice Kirby outlined the pioneering work of multicultural broadcasting in Australia - with cheap programs from all countries reproduced in original languages with TV subtitles. He said that this was a model to be considered in providing cultural diversity.

17. Members of the Group expressed concern about this issue and also about personal alienation caused by the new technology. Television, computer games and the new mode of working in front of a terminal rather than with fellow human beings had reduced the humanity of many people. It threatened the humanity of the workplace in the future. The value of teleconferences was discussed; and whether they would be of the same intellectual and personal value as encounters such as the Salzburg Seminar. Ambassador Marks expressed confidence that the Salzburg Seminar would survive and not be replaced by teleconferences - though these would be useful and cost saving for international negotiations and other highly costly meetings which presently involve the costs and dislocation of long distance travel.

18. Reference was made by one Fellow to the use of telecommunications in court appearances in Canada. Applications for leave to appeal from Vancouver, BC are now made by trans continental teleconference facility rather than the lawyer travelling across the continent for a half hour court session. Justice Kirby mentioned

the use of telephone hook-ups for taking evidence in social security appeals in Australia. The resistance of the legal profession to such innovations was a problem to be watched.

INTELLECTUAL PROPERTY, & BUSINESS LAW

19. The Group then turned to a study of aspects of business law and the way it would need to adapt to the realities of TDF and informatics. Issues discussed included:

- The legitimate needs to protect business confidence;
- The need to adapt intellectual property law (copyright etc) because of the ephemeral nature of the valuable commodity;
- The need to modify trade documentation because of the terms of many Customs laws requiring paper documentation when transational payments may be made by EFT (electronic funds transfer) - involving no paper file at all.
- The potential need for liability insurance against the risk of the breakdown or error of the computer or computer operator. Mention was made of the fee "in" of incorrect data to the plane directional computer which apparently caused the crash of the Air New Zealand jet in Mt Erebus, Antartica in 1979.
- The need for review of the law of computer evidence.
- The need to reconsider conflicts of laws rules in order to determine which legal regime will

apply to a TDF transaction having links with a number of jurisdictions. Whose law is to apply?

INFORMATION SECURITY

20. A number of national data protection (privacy) laws apply rules for securing the safety of personal data. Most information systems owners adopt security systems of their own - but sometimes the law is necessary to enhance the protection offered in this way.

INSTITUTIONS

21. The Group considered the machinery - national and international - for examining the many issues of informatics policy and TDF. The difficulty of getting democratic legislatures of lay persons to consider these complex and sensitive issues was acknowledged. Parliamentary committees face the same problem. The issues are - as one participant described them - "too hot" for legislators. Yet the courts may be too slow and too inexpert. And bureaucrats may not be sufficiently sensitive to the interests involved. Justice Kirby described the work of the Australian Law Reform Commission (ALRC) on privacy protecton, defamation law reform and other issues related to informatics. He stressed the need to help and stimulate the political process to respond to the urgent problems but to do so in an informed way. He mentioned the techniques of the ALRC - in multidisciplinary expertise, public consultation, expert seminars and use of the media to enliven a debate and condition politicians and society

to address the social effects of the new technology.

22. As to international institutions addressing the issues of TDF - the list is long. It includes

CCITT, CoE, EC, GATT, IBI, IIC, INTUG, ITU, OECD, UNCTC, UNCTAD, UNESCO, WIPO and others.

23. Justice Kirby supported the view expressed in Plenary by Mr. John Richardson (EEC), that whilst bilateral negotiation has a place, the very universality of the problems and the scarcity of trained negotiators (especially in developing countries) made the importance and urgency of seeking international solutions obvious. Yet the main initiatives had been taken in OECD and CoE which represent developed countries of the First World. This left a vacuum which needed to be filled - whether by UNESCO, or IBI or some other body so that the multifaceted issues of informatics could be addressed on a global basis - with something like the sense of urgency which is evidence in the technological advances themselves.

OPTIMISM OR PESSIMISM?

24. The Group demonstrated varying degress of optimism and pessimism in respect of the issues and institutional problems brought to light. Some called to attention the warning of Jacques Ellul - "the fact that it is a dictatorship of dossiers rather than of hobnail boots does not make it less a dictatorship". Others were anxious about the dislocations being caused to settled societies by the sudden impact of the new technology. Others were more optimistic. They saw the new technology

as inevitable - thereby requiring us to find solutions to the problems identified. The optimists emphasised the fact that the new technology has a global dimension, tends to spread the flow of information, may yet prove a stimulus to the world economy and will tend to break down barriers of secrecy by the liberating effects of flows of data and the knowledge and power that go with it.

25. Whether the conclusion which our societies will draw will be optimistic or pessimistic will, it was felt, depend in part upon the contributions to be made at home by the participants in the Salzburg Seminar - using the knowledge they acquired in a (mostly) sunny week in one of the most beautiful places on Earth - and resolving to keep the flows of personal data crossing borders between each other in the years to come.

SALZBURG

6 JULY 1985