23rd Australasian Transport Research Forum
Perth, Western Australia 29 September – 1 October 1999

Global Positioning System (GPS) Information and Privacy

Simon Roberts
Department of Infrastructure, Energy and Resources, Tasmania

Abstract

The aim of the paper is to identify the necessary legislative, policy and regulatory changes necessary to address the public's concern about infringement of personal privacy so that GPS information can be utilised by road authorities.

Transport operators are using the Global Positioning System (GPS) for monitoring freight movements and dispatch/fleet management. The use of GPS receivers is growing at such a rate that they are likely to be ubiquitous within a few years. Road authorities in New Zealand, Australia and Europe are positioning themselves to take advantage of the opportunities offered by having GPS technology in an increasing number of vehicles. Issues of privacy and commercial confidentiality relating to the use of GPS information need to be carefully studied. Privacy safeguards should be embodied in the technical design of the system, policy procedures for handling of the information and possible legislative protection against misuse or inappropriate disclosure. Experience in relation to other intelligent transportation systems suggests that it is possible to implement safeguards that adequately address privacy concerns. It is not inevitable that compulsorily gathered data on people's movements will become available for secondary tasks and it is undesirable to allow the benefits of using GPS data to be undermined through a link to state or private surveillance.

Methodology: The paper addresses privacy with reference to established privacy principles first issued by the OECD in 1980 and embodied in the Commonwealth *Privacy Act 1988*. These principles address:

- Collection
- Storage and Accuracy
- Use
- Disclosure
- Public Awareness and Subject Access

The paper identifies inadequacies of the existing policy/regulatory/legislative regime relating to privacy and provides recommendations for enhancement to the existing regime for the purpose of safeguarding privacy under a GPS based road-use information system.

Contact Author
Simon Roberts
Department Infrastructure, Energy and Resources
Level 9, 10 Murray Street
Hobart Tasmania 7000
Phone: +61 3 6233 3091 Fax: +61 3 6233 3091 e-mail: st-robert@dot.tas.gov.au

Introduction

Global Positioning System (GPS) information being gathered by the transport operators for fleet management purposes has value to government agencies. The information could be useful in relation to mass/access management for heavy vehicles, demand management, road planning, allocation of funding and law enforcement. If governments are to reap the benefits of having this information available they must ensure that privacy concerns are adequately addressed. A perception that governments have access to all GPS information and that they may apply it to any purpose could be a serious impediment to the adoption of GPS by fleet managers in Australia.

This paper submits that protection of privacy within any ITS system requires a combination of; technological, legislative, contractual and institutional/administrative measures. The absence of such safeguards in other jurisdictions has resulted in a high level of resistance to the introduction and use of tracking technologies (Alpert 1995).

The Right to Privacy

A recent survey of Australian motorists attitudes (ANOP 1996) found that 'invasion of privacy' was rated among the top two concerns in regard to the introduction of Intelligent Transport Systems (ITS).

The 'right to privacy' was recognised in the *Universal Declaration of Human Rights* (1948) and is reflected in the *International Covenant of Civil and Political Rights* (1966). Australia has applied a number of qualifications to its recognition of a right to privacy in the international arena but the advent of the 'information age' has given the issue a new urgency.

Intelligent Transport Systems have the capacity to collect detailed accounts of road users' activities. There have been attempts by a number of jurisdictions to develop a coherent set of principles governing the collection and use of this information. The principles have been based on privacy principles first codified by the Organisation for Economic Cooperation and Development (OECD 1980) and reflected in the Commonwealth *Privacy Act 1988*.

This paper will examine the applicability of general privacy principles to ITS and assess the success of attempts to tailor the principles to Intelligent Transport Systems. The paper was first prepared as part of Tasmania's *Intelligent Vehicle Trial,* which is investigating the establishment of a GPS based road-use information system by road authorities.

What is 'Privacy'?

The application of ITS to vehicles (and drivers) raises two important issues in the privacy context. Firstly the personal privacy of the driver and, secondly, the business confidentiality interests of transport operators

Protection under existing privacy legislation is only afforded to individuals. In the Commonwealth *Privacy Act 1988*, an individual is defined as a natural person (s6(1)). Personal information is defined as:

> *information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.*

This is a broad definition that has been interpreted as including any information which may allow the identification of an individual (*Re Pfizer* 1993).

Whether positioning information, without combination with other data, will constitute 'personal information' is questionable.

Legislation

Legal privacy safeguards take two forms; legislative and via the common law. In the Commonwealth arena, privacy safeguards are primarily contained in the *Privacy Act 1988*. Other provisions are contained in other statutes but all safeguards relate almost exclusively to information held by Commonwealth Government departments.

Apart from NSW, the states do not have dedicated privacy legislation. There are often, however, provisions relating to specific datasets.

Common Law

While there is no tort of 'invasion of privacy' the court will enforce a right of confidentiality in some circumstances such as doctor-patient or solicitor-client.

Parties to a contract may also impliedly or expressly agree that certain information is to be kept confidential. Such provisions may extend to the protection of all information flowing between the parties to the contract, not just personal information. Breach or threatened breach of such provisions will allow the aggrieved party the usual range of remedies: an injunction against further such breaches, damages or termination.

Inadequacies of Existing Privacy Framework

There are four principal shortcomings of the existing legal framework as it relates to ITS:

1) Narrow application of common law;
2) Lack of legislation relating to state government departments;
3) Lack of legislation relating to the private sector; and
4) Inapplicability of legislation to commercial confidences.

Narrow Application of Common Law

1) None of the recognised relationships giving rise to a presumed right to confidentiality such as doctor-patient or solicitor-client can be applied to the relationship between an ITS provider and user. Although an obligation of confidence can be imputed by the courts in other circumstances it is unlikely that those circumstances would be held to exist in the relationship between ITS provider and user (*Coco* v *Clark* 1969).

2) Broadly drafted contractual provisions requiring non-disclosure of 'confidential information' will generally be ineffective (Littlewoods 1978). Contractual provisions to protect personal information require precise drafting to be effective (Tucker 1990)

3) One must be a party to a contract to enforce a confidentiality provision. This has two implications:
   (a) Unauthorised access to confidential information by a third party will not give rise to an action; and
   (b) Where a data collector and data user have an agreement to keep the information about the data subject confidential, the breach of this provision does not give the person who is subject of the information an action at law.

4) Even if the person who is subject of the information is made party to the contract, breach of confidentiality clause may not result in any quantifiable loss and the action may only result in the award of nominal damages.

Lack of legislation relating to the private sector

The statutory and regulatory coverage of the private sector in relation to privacy is, at best, piecemeal.

The Commonwealth government announced in December 1998 that it would introduce legislation to support and strengthen self-regulatory privacy practices in the private sector, but stated the legislation would represent a 'light-touch' approach (Attorney General 1998). The legislation will be based on the *National Principles for the Fair Handling of Personal Information*, the revised version of which was released in January 1999, by the Office of the Privacy Commissioner.

Inapplicability of legislation to commercial confidences

Privacy legislation does not protect companies or information relating to commercial matters. This can lead to the situation where a sole owner/operator or a partnership may attract the protection of the provision, while the same person or persons operating under an artificial trading structure as a company will not.

Commercial enterprises may reasonably expect that the information collected about their operation be subject to the same privacy protection as information collected about individuals. However, as identified above, privacy safeguards are limited to 'natural persons', and 'personal information'.

Institutional Structures for Collection of Road-use Information by Government

There are three possible models for the collection and use of GPS tracking data by government:

1. Collected and maintained by private operator and audited by government.
2. Collected and maintained by private operator who is certified by government, requiring no government input or auditing. Information required by government may be obtained when devoid of personal identifiers.
3. Information collected, maintained, used and audited by government.

If collected and maintained by government the information will be subject to applicable State and Federal laws. Information custodians would be subject to the Freedom of Information, Archives, and State Service Acts.

The collection of data by the private sector, either by one or a number of companies avoids the fears of 'Big Brother' government surveillance. The private sector is not, however, subject to any form of privacy regulation nor to any code of self-regulatory conduct. Records may still be subject to subpoenas from government or private persons, without any framework determining an appropriate response by the company (for example, the extent to which it should go to prevent the information being accessed) (Gellman 1995)

Privacy Principles

While there is no specific legislation pertaining to ITS systems, Standards Australia have released a set of Privacy Principles for ITS entitled *Australian Privacy Principles for Intelligent Transport Systems* (AAPFITS). Together with the Privacy Commissioner's *National Principles for the Fair Handling of Personal Information* they identify the key privacy concerns raised by the operation of ITS. They can be summarised as follows:

Justification

The Standards Australia principles state that 'there should be strong social justification for any ITS applications which involve any monitoring of an individuals movements'. In a similar vein, the report of the Privacy Committee of New South Wales on Electronic Vehicle Tracking concluded:

In the Committee's view, society should carefully consider whether the benefits this technology promises outweigh the threat to privacy and whether any possible benefits could be gained by alternative, and less privacy invasive, measures. (NSW Privacy Committee 1990)

This principle is partly-flawed in the sense that it views ITS applications as supply driven. As one US expert said " [ITS will become] a way of life primarily because consumers will want its benefits, not because government mandates it or pays for it.

Consumers will be willing to invest in intelligent vehicle highway systems because they want to avoid congestion, have better emergency services, benefit from more convenient routing, and pay tolls where necessary without waiting in line."(Santa Claa 1995)

In this context, it is important that participation in ITS should be voluntary. Any system in which individuals or companies are compelled to be the subjects of surveillance necessitates the strictest possible safeguards to privacy.

The High Court decision in *Johns v Australian Securities Commission* held that where information is *compulsorily* acquired by government, there is a statutory right of confidence. In situations where an individual does not have any choice regarding participation in the collection of data, there may be a restrictive effect on subsequent uses of the information. *Johns* did not restrict its application to Commonwealth government agencies but it is unclear whether this decision has any application to the private sector.

Anonymity

The Standards Australia principles state that, wherever possible, ITS operators should give people the option of entering into transactions which do not require them to identify themselves, and that people using anonymous options should not be disadvantaged (Principle 2).

Anonymous collection of data avoids the accumulation of any individually identifiable information. This would, in an ITS context, include any form of vehicle identification or smart card payment options which could be linked to an individual or company, or information from electronic tags which could be traced to an identifiable bank account.

Many of the functions of ITS are difficult to operate with complete anonymity. For example, electronic tolling of the type found in Melbourne's CityLink is dependent on identifying vehicles (which have tags registered to individuals or companies) in order to charge and prosecute individuals for fare evasion. Identifiable information would also be required to allow individuals or companies to check the accuracy of billing information. Many of the secondary uses of information, such as fleet management, also rely on identifiable information.

The mechanisms by which anonymity can be guaranteed may be technological or institutional. Technical solutions to the issue of anonymity are dependent on the ITS application but generally involve some form of stored-value or debit card and 'digicash'.

Institutional protection for individually identifiable information include the separate storage of identifiers from related information, or the destruction of identifiable information as soon as its purpose is served (for example bills have been sent and verified by the individual). Another option is the use of 'pseudoanonymity'. 'Pseudonymous' transactions involve the recording of a 'pseudo-identifier', and the cross-index between the pseudo and real identifiers are protected by appropriate technical, organisational and legal measures (Clarke 1997)

The real issue, for the current paper, is whether the costs of anonymity should be borne by the individual concerned. Where anonymity (and hence, privacy) is seen as a choice to be made, it creates an opportunity for privacy to become a commercial commodity. I submit that it is undesirable for anonymity to be a commodity that can be sacrificed for commercial gain. For road-users from low socio-economic groups, this may not present a meaningful choice.

Collection Limitation

Principle 3 of *Australian Privacy Principles for ITS* states that:

> *Only minimal amounts of personal information sufficient for the needs of a particular ITS application should be collected by ITS operators. Any such information should be obtained by lawful, fair and non-intrusive means and with the knowledge or consent of the individual involved.*

There is currently no legislation, federal or state, which would adequately ensure compliance with this principle by government or private operators. ITS systems give rise to an opportunity and incentive for operators to collect more information than is necessary for commercial gain or advantage. Serious consideration should, therefore, be given to mechanisms by which the collection of minimum necessary information can be assured.

The weakest mechanism would be a self-regulatory code. While a code may be a useful and positive part of an overall framework, as the sole regulatory mechanism it is insufficient. There is not the incentive to strictly adhere to the policies, nor is there any meaningful recourse for the individual if their privacy is invaded and exploited for commercial gain.

A far stronger mechanism is to legislate to compel companies (or government departments) to avoid the collection of information which is not directly related to the needs of the system and to collect the minimum amount of information required. Legislation of this type should also mandate the data collector notifying the individual as to the exact amount and type of information being collected. This approach lacks flexibility, and poses some problems in defining the parameters of 'minimum'. It does, though, provide a powerful incentive to collect the minimum amount of data possible, particularly where a fine is involved.

A third option is the use of contract between data subjects and data operators. This could specify both the amount and type of information to be collected, and expressly provide that collection should not occur outside these boundaries without the specific consent of the individual. This approach is already in place in some private sector operations (eg mobile phones), and could be easily transferred to ITS operations. However contractual provisions must only be valid where they maintain or increase the degree of privacy protection afforded by legislation.

Data Quality

Data quality relates to security, accuracy, storage and disposal. APPFITS, Principle 7 states that:

> *Information should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.*

Security

Security of data involves technical, physical and organisational safeguards (Gellman 1995). In Tasmania, the Criminal Code provides for the prosecution of persons who have illegally accessed, modified, or destroyed information on a computer. However an additional provision needs to be inserted in the *Code* proscribing the receipt of information so obtained.

One of the greatest risks to data security is abuse of access privileges by authorised users. In the *Melbourne City Link Act 1998 (Vic)*, provisions for a clear audit trail have been made for third party access to the records. There is, however, a far less stringent requirement for audit trails where disclosure or use occurs within the system. Government interference in the ability of private companies to access their own information is problematic. Requiring strict audit trails would, however, emphasise the importance of proper practices regarding information access and aid individuals and companies in identifying improper use of information relating to them.

Storage and Disposal

One mechanism for minimising the improper use or disclosure of information is the prompt destruction of information once its purpose has been served. Given, however, that the department is concerned with the long-term use of roads, this particular method has little utility. Provided also that the department receives information without personal identifiers, the impact of ITS subsequent use and disclosure on the privacy of individuals or companies is far less. There should, however, be some form of legislative framework that provides protection where information is not similarly anonymous.

Records made or kept for the purposes, or in connection with the administration of a Government Department, a State authority, or a local authority, are dealt with under the Archives Act.

Accuracy

Private enterprise and government departments must be required to take all possible steps to ensure that information in the system is accurate and up-to-date.

Legislation may be required to ensure:

- That bodies holding ITS information take all reasonable steps to ensure that the information is accurate and complete before using the information
- That information is not to be used where there is a reasonable suspicion of inaccuracy or incompleteness
- Where a body becomes aware of an inaccuracy or lack of completeness, the record is immediately annotated
- Where inaccuracy or incompleteness have adversely affected an individual or company, some remedy is available

Use & Disclosure

The Purpose Specification Principle (Principle 5) states that:

> *The purposes for which personal information is collected by ITS operators should be specified at the time of collection and the subsequent use limited to the fulfilment of those purposes or other directly related purposes. Personal information collected by ITS operators should be destroyed once it is no longer necessary for these purposes.*

Principle 6 of APPFITS states that:

> *Personal information collected by ITS operators should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the purpose specification principle except:*
>
> *a. with the informed consent of the individual concerned;*
> *b. by the authority of law; or*
> *c. in situations involving serious imminent threat to life or health of the individual concerned or another person.*

Determining the parameters of use of ITS information is a difficult task. The lack of dedicated privacy legislation in Australian States leaves a vacuum regarding enforceable legislative limits on the use or disclosure of information. The High Court decision in *Johns* may be of some assistance in curtailing the indiscriminate use of information acquired by the government, but its scope is uncertain.

Where there is no express legislative protection, information collected by ITS is subject to many legally enforceable disclosure processes (such as subpoenas, law enforcement agencies, regulatory agencies, maybe even private litigants) (Gellman 1995). The use and disclosure of information collected by ITS may therefore significantly exceed that which was originally envisaged (or which was agreed upon by contract).

Clear limits should be placed on the uses for which information may be employed and on the circumstances in which it can be disclosed. This limitation may be made through contract, legislation, or self-regulatory codes. Contract is a particularly useful mechanism by which to establish the parameters of use and disclosure between the individual and the road-operator (although this will only be so where participation in ITS

is voluntary). It may not, however, be effective where the road operator discloses information (legitimately) to a government or law-enforcement agency, which then proceeds to use the information in a manner inconsistent with the purpose of the original data collection.

The CityLink Amendment Act 1998 sets clear legislative limits on the use and disclosure of information for purposes other than toll collection. Tolling information is not to be used or disclosed except in specified circumstances, and its subsequent disclosure and use are regulated to a certain degree (for example, records of disclosure and use must be made, and information disclosed to police can be used for limited purposes) The Ombudsman has also been given jurisdiction to monitor compliance of the police with the requirements of the Act.

The legislation requires
- clear statement of the purposes of the collection
- situations in which disclosure is permitted
- conditions of use and disclosure
- conditions of use and disclosure by third parties
- that the responsibilities and requirements for use and disclosure extend to all those persons, institutions or companies who can access or use the information (for example, subcontractors must deal with information as if they were the primary data collector)
- that consent by the individual or company for uses other than those specified in the legislation must be informed and express

Because legislation is an inflexible tool it is most important that the exact use and disclosures, and policies regarding use and disclosure, are determined in advance of installation of ITS and made clear to the individuals or companies involved in the system.

One of the key concerns is the extent to which information can be used for law-enforcement purposes. In the United States, some private companies discard of information before it can be accessed for law enforcement purposes. In that country there is a belief that law-enforcement should not take precedence over privacy of information collected for road pricing management. Information that could be valuable to law-enforcement agencies may be destroyed before can be used in evidence.

Openness & Individual Participation

The collection of personal and commercial information raises concerns regarding the knowledge of individuals about the nature of information that is held about them and their ability to emend erroneous information.

The regulation of accuracy and access to information will be dependent upon who is holding the information and what form of information is held. Currently, information held by government has protection from third party access and provisions for correction through the Freedom of Information Act 1991. Data held by private companies is not

subject to similar legislative regulation (although in some cases, they enter into contracts with clients to ensure protection and access mechanisms).

The Freedom of Information Act gives individuals a legally enforceable right to be provided with information contained in records in the possession of an agency or Minister unless the information is exempt information under the Act. The disclosure of information which would constitute an 'unreasonable disclosure of information relating to the personal affairs of a person' (other than the person making the request) is exempt from access (as is information provided to government in confidence). The definition of 'personal affairs' has been the subject of considerable debate, but positioning information containing personal identifiers would be likely to attract the operation of the exemption.

Australian FOI Acts allow a person to request an amendment of information if it is incorrect, incomplete, out of date or misleading.

Commercial information which relates to trade secrets, or which would expose a company to competitive disadvantage is also exempt. This exemption has been interpreted narrowly. To avoid this problem some legislation has exempted some commercial information collected by government from the operation of the FOI Act. However, while exemption from the operation of the Freedom of Information Act may be desirable insofar as protecting records from third party access, it does undermine the rights of individuals or companies assessing and checking information, and as such is a problematic mechanism for ensuring the security and confidentiality of records.

Melbourne City Link Amendment Act 1998

The *Melbourne City Link Amendment Act 1998* was passed in late 1998 to address privacy issues related to the Transurban development.

The information being collected by Transurban will be of immense vale to VicRoads for infrastructure planning and demand management. Vicroads have license to collect traffic data in areas of the city other that on the on Transurban roads.

The information could also be of value to police as evidence.

S.90 of the Act defines 'restricted tolling information'. It includes name, address and license plate number of any person or vehicle using the toll zone. It also includes 'any information of a personal nature or that has commercial sensitivity for the person about whom it is kept'.

S90A defines the circumstances under which the information may be disclosed or used. In summary, it may disclosed when reasonably necessary for the collection of tolls and under the circumstances provided in the Standards Australia principle it may also be disclosed at the direction of the Minister. Use or disclosure other than in accordance with s90A incurs a penalty of 100 penalty units or $10,000.

The information may disclosed to police if an officer of the rank of inspector or above requests the information in writing and it related to an indictable offence (the writing requirement may be satisfied by email).

Police are required to retain all records of disclosure for two year and make them available for inspection by the Ombudsman.

In turn, records must be kept relating to any further disclosure of the information by any recipient for a period of two years.

There is no restriction on the amount of information that may be collected by TransUrban. A relatively simple legislative amendment could have been inserted to state that minimum information for the purpose of the collection of tolls would be collected.

There are no provisions in relation to storage and accuracy of the information.

While there are strong provisions in relation to use and disclosure which I have described:

- There is no requirement for an internal audit trail so that an auditor or some other person can determine who is accessing the information internally and why;
- External audit is the responsibility of the Ombudsman who is unlikely to have sufficient resources for the task.
- There are no provisions providing for the inspection and correction of the information.
- There is no requirement for disposal of personal identifiers once they are no longer required. (This is a real issue in the USA where quick disposal of information is a high-priority for users of ITS).
- Finally there is no proscription of collection of the information by non-authorised equipment

Conclusion - Legislative Provisions Relating to ITS

In summary, minimum standards of privacy protection and the methods of collection must be established by legislation. Contractual agreements are valid only where they maintain or increase the degree of privacy protection afforded by legislation. Legislative provisions may be required in relation to the private sector organisations collecting ITS information to ensure that:

- All ITS information collected is confidential, subject only to clearly stated exceptions.
- The data collector will collect the minimum amount of information necessary for the approved uses.
- Approved uses are clearly specified, and more information may only be collected with legislative amendment.

- The data collector provides the person or company concerned with details of:
  - the information that will be collected;
  - authority under which it is collected;
  - clear statement of the purpose of collection and uses to which the information may be applied (and that consent by the individual or company for uses other than those specified in the legislation must be informed and express);
  - circumstances under which the information may be disclosed to a third party and details of third parties to whom information may be so disclosed;
  - responsibilities and requirements of third party recipients of the information;
  - the rights of the data subject in relation to the information (eg: access) and the remedies for wrongful dealing with the information
- Cost of anonymity is not passed on to the individual or company
- Adequate security systems are established and protective measures relating to the form in which the information is kept are implemented.
- A strict regime of audit trails, records and reasons for access, use or disclosure is maintained.
- Non-authorised equipment is not used to collect information from ITS systems. (Gellman 1995)
- That bodies holding ITS information take all reasonable steps to ensure that the information is accurate and complete before using the information and that information is not used where there is a reasonable suspicion of inaccuracy or incompleteness
- Where a body becomes aware of an inaccuracy or lack of completeness, the record is immediately annotated.
- Where inaccuracy or incompleteness has adversely affected an individual or company they have an adequate remedy.
- Companies or individuals have access to information held by private sector data-collectors relating to them.
- A grievance procedure and mechanism by which information can be emended is established.
- That the 'data subject' is informed of changes in relation to persons or organisations that have access to the information;
- That information continues to be secure and subject to correction by the data-subject where the relationship between the data-subject and record-keeper has ceased.
- That the data collector informs the individual or the company regarding the amount and the type of information held about them.
- Receipt or disclosure of the information other than in accordance with these principles is proscribed.

In addition:

- The Freedom of Information Act could be amended to ensure that personal or commercial information collected by ITS systems is protected from third party access (this must be achieved is such a way so as not to undermine the rights of individuals or companies to access information relating to themselves).

References

ANOP, 1996 Survey of Motoring Attitudes to Intelligent Transport Systems, http://www.aaa asn au/anop/its htm

Sheri A. Alpert, 'Privacy and Intelligent Highways: Finding the Right Way, Santa Clara Computer and High Technology Law Journal, vol 11, 1995

'Government to strengthen privacy protection', joint media release, Attorney-Generals and Department of Communications, the Information Economy and the Arts, 16 December 1998, http://www.dcita.gov.au/nsapi-text/?Mival=dca_dispdoc&ID=3416

Roger Clarke, 'Identification, Anonymity and Pseudonymity in Consumer Transactions: A Vital Systems Design and Public Policy Issue', http://www.anu.edu.au/people/Roger.Clarke/DV/AnonPsPol.html

Gellman, 'Privacy and Electronic Clearance Systems', 67

Johns v Australian Securities Commission and Others (1993) 178 CLR 408

OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980

Re Pfizer and Department of Health, Housing and Community Services (1993) 30 ALD 647 at 663

Coco v Clark (Engineers) Ltd [1969] RPC 41, 47 per Megarry J.

Littlewoods Organisation Limited v Harris [1978] 1 All ER 1026, cited in Tucker, *Information Privacy Law*, 39

Privacy Committee of New South Wales, Electronic Vehicle Tracking, Issues Paper No. 62, August 1990

Privacy and ITS, *Santa Clara Computer and High Technology Law Journal*, School of Law, Santa Clara University 1995 pg 5

Tucker, Information Privacy Law, 39