the Copyright Act was amended in 1990 to include Part VA, a statutory licence that allowed educational institutions to copy from television and radio

the people who make and invest in this work so that they will continue to produce programs for our students and teachers.

Since then, the film industry, the education sector, and the copyright landscape has changed dramatically. Video recorders are well and truly outmoded technology – they are large machines gathering dust in the corner. We have digital television, internet streaming, PVRs, retransmission of programs on pay television and mobile phones, electronic whiteboards and online resource centres providing television programs to our educators.

Despite the complexity of this landscape, Screenrights sees the copyright challenge as largely unchanged. How do we ensure access to copyright work while making sure that rightsholders are paid when their work is used? In most cases, this has involved working with both the creators and consumers of content for legislative change that achieves these aims in this new environment.

In the education sector, the change has been particularly dramatic. Teachers and academics are now using new content management systems such as Clickview for their audiovisual collections. Systems such as these let them store, access and play recorded material, and provide digital copies of programs to other schools with the same system. They can show programs to students on electronic whiteboards, and they can also obtain podcasts and vodcasts of their favourite programs from the Internet. In some cases, they are no longer even recording programs themselves. They can go to innovative resources centres, such as RMIT Publishing's Informit, that are making recordings of programs available online to academics across the country.

The Part VA statutory licence has embraced these changes remarkably well. Amendments have allowed for the downloading of certain broadcast material, and for making copied programs available to staff and students online. This has ensured that the licence continues to achieve its two key aims in this new environment: access to copyright users and payment to rightsholders.

Screenrights has also recognised the importance of embracing new technologies to reach the people who are using our members' work. We established EnhanceTV (www.enhancetv.com.au) to let educators know about what's on television and how to use it. Members can subscribe to an online television guide alerting them to upcoming programs relevant to their nominated curriculum areas. They can also download study guides and, now that the site has become a licensed resource centre under Part VA of the Copyright Act, they can obtain copies of programs they forgot to record, or simply ask EnhanceTV to make recordings on their behalf. The service reaches more than 12,000 subscribers on a weekly basis and has recently also become a site where filmmakers and educators can talk to each other, exchanging information and resources to help them teach with television.

The Part VA statutory licence has embraced technical changes remarkably well.

These changes have not only ensured ready access to copyright material for teachers in a technological age, they are also providing a continued growth in copyright income for rightsholders. Last year, more than 45% of the programs copied were documentaries, with the income collected on behalf of these rightsholders helping to ensure that they continue to produce programs that educators want to use.

It's a challenging environment but it's an exciting one. There are not only more opportunities for audiences to enjoy the films and television our members produce, with effective copyright management, there is also a greater number of revenue streams for rightsholders.

Simon Lake is the Chief Executive of Screenrights. More information about Screenrights is available at www.screenrights.org.

Radio Frequency Identification and Data Protection: Privacy and Related Issues

Valerie Perumalla discusses RFID technology and how it fits with regulatory frameworks established by privacy and surveillance legislation.

Location based technologies such as Radio Frequency Identification (**RFID**) are said to pose new threats to security and privacy.[1] Location-based technologies have the potential to enhance the functioning of a range of business operations but there is a growing concern amongst policy makers that certain uses of RFID increase privacy related risks.

A 2006 report issued by the OECD's Directorate for Science, Technology and Industry has called for further discussion amongst policy makers on the future of RFID:

> The window of opportunity is now, for policy makers, industry and consumers to understand and discuss forward-looking public policy issues associated with radio frequency identification technology and applications, as well as to review existing and proposed associated legislation.[2]

Similarly, numerous academics have suggested that location technologies have far outstripped both public awareness and legal and policy attention.[3]

There is no Australian legislation that directly addresses RFID technology, but where 'personal information' is concerned the Privacy Act 1988 (Cth) (**Privacy Act**) comes into effect regardless of the specific technology used for collecting that information. Certain uses of the technology may also be incidentally regulated. The Surveillance Devices Act 2007 (NSW) was developed primarily to regulate law enforcement agencies, but may restrict commercial uses of RFID where the technology conforms to the definition of a 'tracking device'.

Definition of RFID

RFID is used in a wide range of applications and the impact on personal privacy and data protection varies depending on the specific system and its application. Inexpensive RFID tags used for basic object identification typically consist of a tiny electronic circuit attached to a small antenna that is capable of transmitting a unique serial number to a reader.[4] More complex forms of RFID technology include contactless cards, used, for example, for access control, individual identification (passports and electronic ID cards), digital keys (vehicles or motels), or payment.[5] RFID may be considered as one of a group of automatic identification and data capturing technologies which also includes bar codes, biometrics, magnetic stripes, optical character recognition, smart cards, voice recognition and similar technologies.[6]

The privacy risks of automatic identification and data capturing technologies are exacerbated when they are combined. For example, RFID may be combined with biometric technology to create an e-passport (RFID as part of a personal identification system or passport generally involves scanning and recording a biometrically unique feature of a person and encoding this data digitally on an RFID chip for later retrieval and analysis during an authentication process).[7]

Commercial applications of RFID

RFID has been used for many years in transport, access control, event ticketing and management, more recently in government identity cards and passports and extensively in manufacturing supply chains and in logistics for goods distribution.[8] The most significant use of RFID technology in Australia is in supply chain and inventory management. The more advanced or high-end RFID systems can be interfaced with sensor networks, which can actively capture and record information about their surroundings.[9] Such information includes the temperature; the composition of the atmosphere; exposure to chemicals; and quantities and measurements of materials.[10] This information can be used to aid business processes such as quality assurance in manufacturing, climate control in horticulture, and the management of storage conditions for hazardous materials.[11]

The Organisation for Economic Co-operation and Development (**OECD**) has identified eight fields of RFID application.[12] The most prominent applications are in the tracking, assembling and manufacturing of products within the supply chain.

Asset utilisation

Mobile assets are tagged for their use along the supply chain. Typical examples are RFID tagged containers which are used at different production stages. Companies rely on RFID technology in order to locate these assets and to monitor which departments use the assets how many times. The aim is to optimise processes and attain a more efficient use of capacity.

Asset monitoring and maintenance

Mostly fixed and high value assets are tagged to store information, e.g. for maintenance purposes. Examples include tagged machines where the maintenance history and information on replaces parts are stored in the tag.

Item flow control in processes

For item flow control, RFID tags are attached to items which are moving along the supply chain. Often information going beyond a simple ID number is stored on the tag to control production processes. This is, for example, the case in the automotive industry where production information is stored on the tag which can be attached to car bodies or smaller parts.

Inventory audit

A prominent application is the use of RFID for inventory audit. Examples include retailers, warehouses where pellets and sometimes cases are tagged to improve the speed and efficiency of stock taking.[13]

Australian legislation and RFID

The Australian Law Reform Commission (**ALRC**) conducted an inquiry last year on the extent to which the Privacy Act and related legislation continue to provide adequate protection of privacy in Australia. The ALRC's report, For Your Information: Australian Privacy Law and Practice, expressed concerns about RFID technology use, in particular, the ability of agencies, organizations or persons to track individuals as they walk in places (airports, train stations, stores), and monitor consumer behaviour in stores.[14]

The ALRC also indicated that the potential for an RFID setup to be accessed by unauthorised users has led to technological developments that aim to prevent the unwanted scanning of RFID tags, such as 'blocker tags' which impair readers by simulating the signals of many different RFID tags.[15] The ALRC took the view that it is not practical to encourage individuals to purchase and carry 'blocker tags'.[16]

Surveillance Technology and RFID

Certain uses of RFID may amount to surveillance. Surveillance involves the monitoring of a person, place or object to obtain certain information or to alter or control the behaviour of the subject of the surveillance. [17]

Surveillance technology has traditionally been used by law enforcement agencies to prevent or investigate crime and by media organisations pursuing news. The primary legislation regulating the use of surveillance devices in New South Wales is the Surveillance Devices Act 2007 (Cth) (**Surveillance Devices Act**).

Section 9 of the Surveillance Devices Act could affect RFID use. The section prohibits the installation, use and maintenance of tracking devices on a person, or an object that a person is in possession or in control of, without that person's consent. The section would not prevent the use of RFID technology to track objects within a supply chain. However, once a tracked object is sold to a customer and that object or a person in possession of that object is **capable** of being tracked by an RFID reader without his or her consent, section 9 of the Surveillance Devices Act would appear to be contravened.

Whether RFID conforms to the definition of a 'tracking device' depends on how RFID is used and if it is used in compliance with spectrum licensing arrangements set by the Australian Communications and Media Authority (**ACMA**). As observed by the Department of Communications, Information Technology and the Arts:

> The spectrum licensing arrangements by ACMA for RFID equipment specify the power at which equipment can be used, and as a consequence the read range. This effectively prevents the tracking of tags and the objects or people carrying them over wide areas.[18]

Whether RFID conforms to the definition of a 'tracking device' depends on how RFID is used and if it is used in compliance with spectrum licensing arrangements set by the ACMA.

However, there are concerns that it is not possible to predict read ranges. A read range is the distance at which a reader device can effectively read information from an RFID tag. Depending on the power and technical specifications of the equipment being used, this can vary from a few centimetres or a few metres, to up to 100 metres.[19] The effective read range of an RFID system is dependent on many factors, notably:

- Transmitting power generated by the reader.
- Environment (indoor/outdoor).
- Susceptibility to noise and interference from other radio devices.[20]

As a result, read ranges have to be considered as approximate values.[21]

Certain uses of RFID may amount to surveillance.

The Privacy Act

The Privacy Act sets out 10 National Privacy Principles (**NPPs**) which regulate how businesses collect, handle, store, use and disclose personal information. The ALRC has indicated that the handling of personal information obtained by the use of surveillance devices is generally regulated by the Privacy Act, when the use of the device involves the collection of personal information for inclusion in a record.[22]

'Personal Information' as defined by the Privacy Act means:

> 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.[23]

The key question raised by this definition is whether or not the identity of a person can be reasonably ascertained from the information transmitted, used or stored by an RFID tag. The monitoring of consumer behaviour itself, so long as a person cannot be identified from the information collected, is not affected by the Privacy Act. Further, the commercial applications of RFID discussed above are unlikely to involve the collection of personal information with the exception of e-passports. An RFID tag, in and of itself, is not sufficient to identify a person unless RFID technology is used to store and process personal data.

Traditional data protection legislation should be extended to specifically address RFID technology in order to keep up with the growing use of RFID technology in Australia

DCITA Guide to RFID

In 2006, the Department of Communication, Information Technology and the Arts issued a guide, Getting the Most Out of RFID, which was prepared in consultation with the RFID Association of Australia. The guide intended to give small to medium size enterprises practical advice on the benefits of RFID, and also outlined some of the issues that should be considered when adopting the technology. Relevantly, the paper called for small to medium-sized enterprises to put in place a privacy impact statement and noted a number of privacy principles suggested by Privacy Commissioners around the world in relation to RFID. These principles include:

- RFID tags should only be linked to personal information or used to profile customers if there is no other way of achieving the goal sought;
- Individuals should be personally informed if personal information is collected using RFID tags;
- Personal information collected using RFID tags should only be used for the specific purpose for which it is first collected, and destroyed after that purpose in achieved; and
- Individuals should be able to disable or destroy any RFID tag that they have in their possession.[24]

Conclusion

While there is no specific privacy regulation of RFID systems by governments in Australia, there is general legislation applying to all forms of businesses including the commercial use of RFID. [25] Traditional data protection legislation should be extended to specifically address RFID technology in order to keep up with the growing use of RFID technology in Australia.

Valerie Perumalla is a student at UTS. This essay was highly commended in the 2009 CAMLA essay competition.

(Endnotes)

[1] See Katherine Albrecht and Liz McIntyre Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID (2006).

[2] OECD Radio-frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations Doc DSTI/ICCP (2006) 5.

[3] See Roger Clark and Marcus Wigan 'You Are Where You Have Been' in Katina Michael and M.G Michael (eds) Australia and the New Technologies: Towards Evidence Based Policy in Public Administration (2008) 155, 155.

[4] OECD Radio-frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations Doc DSTI/ICCP (2006) 7.

[5] Ibid.

[6] OECD Radio Frequency Identification: OECD Policy Guidance, A Focus on Information Security and Privacy Applications, Impacts and Country Initiatives OECD Ministerial Meeting on the Future of the Internet Economy, Seoul, Korea (17-18 June 2008) 3.

[7] J.M. Stanton, 'ICAO and the Biometric RFID Passport' in Colin Bennet and David Lyon (eds), Playing the Identity Card: Surveillance, Security and Identification in Global Perspective (2008) 250, 253.

[8] Ibid.

[9] Department of Communications, Information Technology and the Arts Getting the Most out of RFID: A Guide for Small to Medium Sized Enterprises (2006) 6.

[10] Ibid.

[11] Ibid.

[12] OECD Radio Frequency Identification: OECD Policy Guidance, A Focus on Information Security and Privacy Applications, Impacts and Country Initiatives OECD Ministerial Meeting on the Future of the Internet Economy, Seoul, Korea (17-18 June 2008) 97.

[13] Ibid.

[14] Australian Law Reform Commission For Your Information: Australian Privacy Law and Practice Report No 108 (2008) [9.41].

[15] Ibid 9.42.

[16] Ibid.

[17] Ibid 9.89.

[18] Department of Communication, Information Technology and the Arts Getting the Most out of RFID: A Guide for Small to Medium Sized Enterprises (2006) 21.

[19] Ibid 37.

[20] OECD RFID implementation in Germany: Challenges and Benefits Doc DSTI/ICCP (2007) 11-12.

[21] Ibid 12.

[22] Australian Law Reform Commission For Your Information: Australian Privacy Law and Practice Report No 108 (2008) [9.94].

[23] Privacy Act 1988 (Cth) s 6.

[24] Department of Communication, Information Technology and the Arts Getting the Most out of RFID: A Guide for Small to Medium Sized Enterprises (2006) 21.

[25] Ibid 20.