

INTERIM REPORT

**FOR THE CONTENT AND RIGHTS WORK
PACKAGE (CR6)**

**DATASET ACQUISITION, ACCESSIBILITY AND
ANNOTATION e-RESEARCH TECHNOLOGIES
PROJECT (DART)**

David Lindsay

Ann Monotti

Moira Paterson

Anne Chin

Faculty of Law, Monash University

23 January 2007

PREFACE

This is the Interim Report for the Content and Rights work package (CR6) which forms one of a number of work packages that comprise the Dataset Acquisition, Accessibility, and Annotation e-Research Technologies Project (DART). The aim of work package CR6 is:

‘to improve content deposit rates by clarifying legal issues around intellectual property, information security and privacy.’

As the research for this work package progressed, it became obvious that the production of a final report by December 2006 was not feasible for the following reasons:

1. There were too many uncertainties surrounding the way in which DART might support e-Research; and
2. Each of the demonstrator models remains in a state of flux. This makes it impossible to clarify legal issues in the way that was proposed when the research commenced in January 2006.

As a result of these uncertainties, we have produced this Interim Report.

The Interim Report comprises an Executive Summary followed by chapters that explain the nature of e-Research, the DART project itself and the legal issues that arise in the areas of intellectual property law, the law of privacy and freedom of information, and information security law.

The Executive Summary includes a number of specific questions that seek information and guidance. A final report will issue at the end of June 2007 that will take into account the information we receive in response to both those specific questions and the general content of the Interim Report.

We request that the Interim Report be circulated to all Chief Investigators and all other relevant persons for the express purpose of providing us by no later than 31 March 2007 with further information and guidance.

We request that the Interim Report be circulated to all Chief Investigators and all other relevant persons for the express purpose of providing us by no later than 31 March 2007 with further information and guidance.

Acknowledgments

The authors of the Interim Report would like to thank those DART researchers who have assisted with the report by answering our numerous requests for information about what they are doing. In particular, we would like to thank Jeff McDonald, who was the DART project manager for the period in which this report was produced, and Andrew Treloar, who was instrumental in establishing the DART project. This Interim Report would not have been possible without the diligent work of our research assistant, Anne Chin, for which the other authors are grateful.

Responsibilities

The authors of the report are jointly responsible for all of the material included in the Interim Report. Nevertheless, individual authors had primary responsibility for those chapters which reflect their areas of particular expertise. Thus, Ann Monotti had primary responsibility for chapter 4, which deals with intellectual property issues; Moira Paterson had primary responsibility for chapter 5, which deals with privacy law and freedom of information; and David Lindsay had primary responsibility for chapter 6, which deals with information security law. The authors each contributed material to chapter 1, which deals with e-Research, and chapter 2, which explains the DART project. Anne Chin provided indispensable research assistance for the project, and made contributions to each of the chapters.

Mr David Lindsay

Associate Professor Ann Monotti

Associate Professor Moira Paterson

Ms Anne Chin

23 January 2007

AUTHOR BIOGRAPHIES

Mr David Lindsay BA LLB (Syd) LLM (Melb)

Email: david.lindsay@law.monash.edu.au

Webpage: <http://www.law.monash.edu.au/staff/dlindsay.html>

David Lindsay is a Senior Lecturer at Monash Law School, with expertise in intellectual property law, privacy law, Internet and e-commerce law, and electronic communications law and regulation. He is a co-author of *Copyright and Designs* (Butterworths, Sydney, 1996-), a major reference work on Australian copyright law, and author of a forthcoming text on *Domain Name Governance and Dispute Resolution* (Hart Publishing, London, 2007). David has published many peer-reviewed articles and book chapters in the areas of privacy law, copyright law, Internet law, telecommunications law and broadcasting law. He is a member of the editorial boards of the *Australian Intellectual Property Journal*, the *Media + Arts Law Review* and the *Privacy Law + Policy Reporter*.

David has presented many papers at Australian and international conferences in the areas of intellectual property law, privacy law, Internet law, and broadcasting and telecommunications law. He has written substantial consultant's reports dealing with telecommunications codes of practice and copyright licensing. As a Senior Fellow at Melbourne Law School, from 1999-2002, he conceived and wrote a series of monographs on Internet law and policy, dealing with issues relating to Internet censorship, defamation, copyright liability and technological protection measures (TPMs). He was also responsible for organising a series of seminars on Internet law, and for coordinating the Australia consultation for the Second WIPO Domain Names process. David is currently in the final stages of a doctorate addressing problems relating to the protection of privacy in the on-line environment.

Associate Professor Ann Monotti (Hons) LLM (Melb) PhD (Mon)

Email: ann.monotti@law.monash.edu.au

Webpage: <http://www.law.monash.edu.au/staff/amonotti.html>

Ann Monotti is the co-author of the book *Universities and Intellectual Property, Ownership and Exploitation* (Oxford University Press, Oxford, 2003). The book was submitted as the author's PhD and is held in libraries throughout the world, including the Universities of Oxford, Cambridge, Stanford, and Harvard. Over the past five years, she has delivered papers in the Netherlands, Washington DC, USA, London, Oxford and Newcastle, UK. Ann has published widely in Australian and international refereed journals on intellectual property related issues, most recently in the field of patent law and access to tangible research materials in biomedical research. She has been cited by various members of the judiciary in both the Federal Court of Australia and the South Australian Supreme Court, in Australian and international texts, refereed journals including the *Federal Law Review*, the *Sydney Law Review*, the *Stanford Law Review* and the *International Review of Intellectual Property and Competition Law*, and by law reform bodies including the Australian Law Reform Commission and the Copyright Law Review Committee. She is an Australian correspondent for the *European Intellectual Property Review* and a member of the Editorial Board for the *International Journal of Information Policy and Law*. From 2003 – 2006, Ann was a member of the 'Zwolle Group'. This international group, comprising representatives of authors, publishers, librarians, law academics and universities, was formed following the inaugural meeting that the SURF Foundation organized in Zwolle, The Netherlands in 2003. The Zwolle Group has worked with academic authors, institutions, publishers and libraries to produce a number of outcomes including the 'Zwolle Principles' that seek to provide optimal access to scholarly information. Its activities were supported and sponsored by both the SURF Foundation in The Netherlands and JISC in the UK.

Ann is the Associate Dean (Postgraduate Studies), having formerly occupied the positions of Associate Dean (Research) and Director of Higher degrees by Research in 2004. She is a member of the Intellectual Property Committee of the Law Council of Australia. She has won two ARC large grants to pursue research in relation to universities and ownership of intellectual property and access to and protection of biomedical research materials. She is a Chief Investigator in the DEST funded Dataset Acquisition, Accessibility and Annotation e-Research Technologies Project (DART). Prior to embarking upon an academic career in 1991, Ann was a partner in the legal practice F R Monotti and Co.

Associate Professor Moira Paterson BEc LLB (Hons) LLM GDHE PhD (Mon)

Email: moira.paterson@law.monash.edu.au

Webpage: <http://www.law.monash.edu.au/staff/mpaterson.html>

Moira Paterson is the author of the book *Freedom of Information and Privacy in Australia: Government and Information in the Modern State* (LexisNexis/ Butterworths, 2005). Moira has published several chapters in books and major reference works and numerous refereed articles on freedom of information, privacy, health records and intellectual property related issues. She has also presented many papers on freedom of information and privacy related issues at local and international conferences. Her work has been cited in various cases including decisions by the Constitutional Court of South Africa, the Federal Court of Australia and the New South Wales Court of Appeal and in local and international refereed journals including the *Federal Law Review*, the *Melbourne University Law Review*, the *University of Toronto Law Journal*, the *John Marshall Journal of Computer and Information Law*, the *International Journal of Human Rights and the Comparative Labor Law and Policy Journal*, and by law reform bodies including the Administrative Review Council, the Victorian Law Reform Committee and the Singapore, National Internet Advisory Committee.

Moira is member of the Advisory Committee to the Australian Law Reform Commission in relation to its review of the Privacy Act 1988 (Cth), a member of the Privacy Roundtable for the National Electronic Health Transition Authority and FOI Editor of the *Australian Administrative Law Service*. She was a consultant to Public Accounts and Estimates Committee of the Victorian Parliament in relation to its report *Commercial in Confidence Material and the Public Interest* (2000) and a member of the Expert Advisory Committee on Privacy to the Victorian Law Reform Commission in respect of its *Workplace Privacy Issues* paper.

Within Monash Moira is the Honours Convenor for the Law Faculty, a legal member of the University Standing Committee on Ethics in Research Involving Humans and member of the Committee for the Monash E-health Research Unit. She is a Chief Investigator in the DEST funded Dataset Acquisition, Accessibility and Annotation e-Research Technologies Project (DART) and was previously a Chief Investigator for a multidisciplinary team project funded by an ARC large grant to investigate the legal, ethical and record-keeping issues raised by shared electronic health records system. Her primary areas of expertise are in the fields of privacy, health records and access to information.

Ms Anne Chin BSc (Hons)/LLB (Hons) Grad Dip Legal Practice

Email: ann.chin@law.monash.edu.au

Anne Chin is a Research Assistant at Monash Law School who has been working exclusively on the DART project. During her work on the DART project, Anne has assisted in the completion of an article with her supervisors that has been accepted for publication, 'DART: A new missile in Australia's e-research strategy'.

Anne was admitted to practice as a Barrister and Solicitor of the Supreme Court of Victoria upon completion of a Graduate Diploma in Legal Practice in 2004 at the Leo Cussen Institute. After being admitted, Anne worked as a first year solicitor at Stephens Lawyers and Solicitors, where she practiced in areas such as trade marks, trade practices and patents. Anne completed her Bachelor of Science (Honours) and Bachelor of Laws double degree at Monash University. During her Law degree, she completed an Honours thesis on the regulation of organ and tissue transplantation in Australia. In addition, Anne completed an Honours year in Science, majoring in Pharmacology, where she conducted laboratory and literary research to produce an Honours thesis on cardiovascular regulation in the brain. Anne will commence a PhD in 2007 at the Monash Law School concerning open source software in collaborative projects.

TABLE OF CONTENTS

PREFACE	ii
AUTHOR BIOGRAPHIES	iv
1 Executive Summary	1
1.1 e-Research	3
Issues for Discussion	4
1.2 The DART project.....	5
Issues for Discussion	6
1.3 Intellectual property	7
Issues for Discussion	8
1.4 Privacy and Related Laws	10
Issues for Discussion	11
1.5 Information Security	12
Issues for Discussion	13
2 THE DEVELOPMENT OF e-RESEARCH	15
2.1 Introduction	15
2.2 The Evolution of e-Research	15
2.2.1 Background	15
2.2.2 Developments involving the Internet and the World Wide Web	17
2.2.3 Grid computing	18
2.2.4 The New e-Research Projects	19
2.2.5 Key Developments	20
2.2.6 Europe.....	20
2.2.7 United States.....	21
2.2.8 Canada	22
2.2.9 Australia	23
2.3 the DART Project	24
2.4 The next stage: the ARCHER project.....	25
2.5 Summary.....	28
3 THE DART PROJECT	34
3.1 Introduction	34

3.2	The DART project work package groups	36
3.2.1	Storage and Interoperability (SI)	37
3.2.2	Content and Rights (CR).....	38
3.2.3	Annotation and Assessment (AA)	39
3.2.4	Discovery and Access (DA)	40
3.3	DART Demonstrator Models	41
3.3.1	X-Ray Crystallography Demonstrator Model	41
3.3.2	Climate Research Demonstrator Model	48
3.3.3	Digital History Demonstrator Model.....	50
4	INTELLECTUAL PROPERTY.....	57
4.1	COPYRIGHT.....	57
4.1.1	Introduction	57
4.1.2	Legal protection	58
4.1.3	Subject Matter	59
4.1.4	Criteria for protection.....	60
4.1.5	Authorship of works and the maker of other subject matter 61	
4.1.6	Ownership of works and other subject matter.....	63
4.1.7	The exclusive rights of copyright	66
4.1.8	Moral rights	69
4.1.9	Performers' Rights.....	70
4.1.10	Duration of copyright protection	71
4.1.11	Infringement of Copyright	73
4.1.12	General comments about copyright and the e-Research process 78	
4.2	Copyright issues arising at specific stages of the e-Research process 80	
4.2.1	The Data Collection, Monitoring and Quality (DMQ) Assurance work packages (DART DMQ packages)	80
4.2.2	Transfer and storage of data (DART SI packages)	82
4.2.3	The submission of data and results by researchers into repositories (CR packages)	84
4.2.4	Annotation and assessment of research data (AA work packages)	85
4.2.5	Discovery and Access (DA work packages).....	88

4.3	PROTECTION OF CONFIDENTIAL INFORMATION: The equitable doctrine of breach of confidence	89
4.3.1	Identification of the Information	91
4.3.2	Quality of Confidence	91
4.3.3	Circumstances that Import an Obligation of Confidence ...	91
4.3.4	Misuse of Information	91
4.3.5	Detriment	92
4.3.6	Defences	92
4.4	Confidentiality issues arising at specific stages of the e-Research Process	92
4.4.1	Collection of identifiable personal information via remote instruments (DART DMQ packages)	92
4.4.2	Transfer and storage of data (DART SI packages)	93
4.4.3	The submission of data and results by researchers into repositories (CR packages)	94
4.4.4	Annotation and assessment of research data (AA work packages)	95
4.4.5	Discovery and Access (DA work packages)	96
4.5	PROTECTION OF CONFIDENTIAL INFORMATION: The equitable doctrine of breach of confidence	100
4.5.1	Identification of the Information	102
4.5.2	Quality of Confidence	102
4.5.3	Circumstances that Import an Obligation of Confidence .	103
4.5.4	Misuse of Information	103
4.5.5	Defences	103
4.5.6	Confidentiality issues arising at specific stages of the E-Research process	104
(i)	Collection of identifiable personal information via remote instruments (DART DMQ packages)	104
(ii)	Transfer and storage of data (DART SI packages)	105
(iii)	The submission of data and results by researchers into repositories (CR packages)	105
(iv)	Annotation and assessment of research data (AA work packages)	106
(v)	Discovery and Access (DA work packages)	107
5	PRIVACY AND RELATED LAWS.....	113

5.1	PRIVACY	113
5.1.1	Introduction	113
5.1.2	Legal protection	113
5.1.3	Information privacy laws	114
5.1.4	Health Records laws	122
5.1.5	Anti-surveillance laws	124
5.1.6	Common law	124
5.1.7	Privacy Issues Arising at Specific Stages of the e-Research Process	125
5.1.8	Some more complex privacy issues raised by the DART project	134
5.2	FREEDOM OF INFORMATION.....	138
5.2.1	Some more complex FOI issues raised by the DART project	145
5.3	ARCHIVES/PUBLIC RECORDS LEGISLATION	146
5.3.1	Some more complex public records issues raised by the DART project.....	148
6	INFORMATION SECURITY.....	150
6.1	Introduction	150
6.2	Objectives of information security	151
6.3	Techniques for safeguarding information security	152
6.3.1	Information security fundamentals.....	153
	Figure 6.5 - Asymmetric cryptography with digital signature	158
6.3.2	159
6.4	Information security initiatives.....	162
6.4.1	Globus Grid Security Infrastructure (GSI)	162
6.4.2	Shibboleth.....	164
6.4.3	The Australian Higher Education eSecurity Framework...	167
6.5	Security Policies and Procedures	170
6.6	Principles of legal liability for information security systems and security breaches	172
6.6.1	Participants in e-Research transactions.....	173
6.6.2	Sources of legal liability.....	174
6.6.3	Liability in negligence.....	175
6.6.4	Trans-border issues	178

APPENDIX 1	183
Legal liability of participants in e-Research transactions for information security systems and for security breaches	183
PKI	183
Shibboleth system.....	188
APPENDIX 2	194
Glossary	194
APPENDIX 3	203
Acronyms and Research Initiatives	203

1 EXECUTIVE SUMMARY

This is an *Interim Report* that forms one part of the Content and Rights work package (CR6) of the DART project.

The scope of the *Interim Report* is limited. Its aim is to *identify* the most important legal issues that arise from the DART project, and from the new e-Research environment more generally. It does not attempt to *analyse* the legal issues. Nor does it make recommendations about how to resolve the identified problems. The report was always designed to be limited in this way, as it was envisaged that a considered legal analysis, and the formulation of recommendations for resolving legal issues, would be impossibly ambitious within the DART time-frame. Given the scale of the DART project, the identification of the most important legal issues has, in itself, been ambitious. At the same time, the research undertaken in producing this report has confirmed that the analysis of the legal issues, and the development of recommendations for dealing with the problems, deserves serious future research attention.

The DART project is an integral part of a new generation of e-Research initiatives, both in Australia and internationally, that have the potential to transform university research. The *Interim Report* clarifies that the differences between the emerging e-Research environment and the previous environment create new legal issues. The report also confirms that legal problems that exist with current research practices will become more prominent in the new environment.

If e-Research is to fulfil its true potential, researchers must be satisfied that the benefits of involvement outweigh any associated risks. A prime area of risk involves legal issues that escalate into disputes that involve lengthy and costly resolution. Minimisation of this risk is only possible after identification of the potential legal problems that might arise within the e-Research environment.

The legal problems arise mainly because e-Research facilitates new forms of remote research collaboration across institutions, across national borders and across academic disciplines. Importantly, the new forms of collaboration can involve researchers with no established legal or research relationships. Where people with no established relationships interact in important activities

there is a potential for legal disputes. The potential for legal disputes is greater where the applicable law is ambiguous or unclear.

The *Interim Report* identifies legal problems in three main areas:

- intellectual property law;
- privacy and freedom of information; and
- information security law.

The selection of these three areas was made after an initial survey of all potential legal issues that could be relevant. But it should not be taken to mean that the new e-Research environment does not give rise to potential problems in areas of the law that are not covered by the report. The authors, however, are satisfied that, by concentrating on these three areas, we have identified the most important issues that are likely to arise in practice.

As our research progressed, we formed the view that it was essential to obtain feedback on our work from researchers that are involved with the DART project. The DART project is so ambitious and complex that it is impossible for us to be familiar with all aspects of the project. Moreover, DART is very much a 'work in progress', with important aspects of the project being developed and updated as we are writing.

This Executive Summary therefore summarises the results of our research to date and seeks feedback on particular research questions (known as '*Issues for Discussion*'). The questions set out in the Executive Summary are designed to guide the feedback requested from DART researchers. You should not, however, feel constrained by these questions in providing feedback. The authors will appreciate all comments or feedback on any aspects of the *Interim Report*. In particular, readers should note that the substantive chapters of the report include specific examples of the sorts of legal problems that we think may arise in practice.

We would appreciate any feedback on whether researchers consider these hypothetical problems are likely to arise, and on whether there are any other practical problems that you think should be addressed by the *Final Report*.

1.1 E-RESEARCH

Proper appreciation of the legal problems associated with the DART project requires an understanding of the emerging new e-Research environment, and the place of DART within this new environment. This is explained in Chapter Two of the *Interim Report*.

The international research landscape is increasingly being shaped by two inter-related developments:

- an increased commitment on the part of governments (and others) to the promotion of open access to information; and
- continuing innovations in information and communication technologies (ICTS).

Together, these developments create the potential for new forms of research collaboration and information sharing.

An initial series of projects, involving the development of institutional repositories for the sharing of published data and other research outcomes, has been followed by a new wave of projects that go further. In particular, the new projects involve the development of the infrastructure needed to share the data that forms the raw material for research in the sciences, and many of the social sciences. In Australia, the DART project (followed by the ARCHER project) is pioneering this new wave of developments.

The new e-Research infrastructure, which is being built in Europe, North America and Australia, will create a new research paradigm which is increasingly international, collaborative and interdisciplinary. The emergence of this new paradigm should increase the rate, quality and efficiency of innovative university research, especially in areas that involve the production and use of large data pools.

The DART project is an important contribution to the new e-Research environment. A feature of DART that distinguishes it from other e-Research infrastructure projects is that it takes a 'whole process' approach to e-Research. This means that the project addresses all stages of the research process: starting with information creation; through processing, exchange, use and management of the information; and including publication of research outputs. The 'whole process' approach adopted by DART gives rise

to more legal issues than other, less ambitious, e-Research projects, such as those aimed at establishing repositories for published materials.

Given the importance of understanding DART within the context of broader developments within e-Research, the authors request feedback concerning the accuracy of our understanding of the emerging e-Research environment, and the way in which DART fits within the broader e-Research landscape.

Issues for Discussion

Feedback from DART researchers is requested in relation to the following matters:

Question 1.1

Do you agree with the description of e-Research set out in the Interim Report, and the way in which the report distinguishes the new e-Research environment from existing research practices? Are there any important omissions in our understanding of the new e-Research paradigm?

Question 1.2

Are you aware of important e-Research projects, or other initiatives, that you believe should be included in the final report?

Question 1.3

Are the descriptions of the DART and ARCHER projects included in this chapter of the report accurate and complete?

1.2 THE DART PROJECT

The DART project is explained in Chapter Three of the *Interim Report*.

The DART project aims to provide tools and services for collaborative research across the entire e-Research process, from the creation and collection of raw data, to the publication of research. As such, it is designed to provide a system that: deals with large-scale data collection from various sources; provides for the storage of a variety of digital objects in repositories; and allows researchers to analyse, annotate and publish stored data.

The DART project consists of five sets of work packages which each reflect a stage of the e-Research process.

1. A set of *Data Collection, Monitoring and Quality Assurance (DMQ)* packages which involve the investigation of issues concerning the collection, monitoring and quality of large data streams, including the requirements involved in dealing with large streams of data created at a high rate via the linkage of instruments and sensors to remote users and collection facilities.
2. A set of *Security and Interoperability (SI)* packages focussing on the security and accessibility of a range of digital objects, including issues associated with the collection of data from devices, the security of data during transfer between networks, the storage of data on high-capacity devices, the preservation and management of data in repositories and ensuring the integrity of data.
3. A set of *Contents and Rights (CR)* packages that examine methods, technologies and incentives to address researchers' concerns in relation to submitting their research and data into institutional repositories.
4. A set of *Annotation and Assessment (AA)* packages focussing on establishing tools and services that will allow users to attach opinions, reviews, comments or assessments to research data, publications, reports and other digital objects stored in DART repositories.

5. A set of *Discovery and Access (DA)* packages involving the development of tools and services that allow users to browse, search, discover and access resources within repositories.

The DART project incorporates three Demonstrator projects in the areas of Crystallography, Climate Research and Digital History. These projects have been chosen to highlight how the tools established by the DART work packages can be used in practice in the science and humanities disciplines, and to provide a 'proof of concept' for the new research tools.

It is extremely important for the analysis of the legal issues associated with the DART project to be based on a precise and accurate understanding of the project, and of the demonstrator models. The changes that have necessarily been made in some of the DART work packages, and in the demonstrator models, during the course of the project have created difficulties for our research. We therefore rely upon feedback from DART researchers to provide us with as accurate a picture of the work packages included in the DART project as possible.

Issues for Discussion

Feedback from DART researchers is requested in relation to the following matters:

Question 2.1

Is the description of the DART project (and the individual work packages) set out in this chapter accurate and complete?

Question 2.2

Have there been important developments in the work packages that need to be drawn to our attention, so that the final report can deal with them appropriately?

Question 2.3

Is the discussion of the Demonstrator Models included in the chapter accurate, complete and up to date?

1.3 INTELLECTUAL PROPERTY

The main legal issues associated with some aspects of intellectual property law are explained in Chapter Four of the *Interim Report*.

All the creative products of those who are involved in academic research are capable of legal protection under one or more of the areas of intellectual property (IP) law. These areas are known as copyright, patents, designs, trade marks, circuit layouts, plant breeder's rights and the equitable doctrine of breach of confidence. This chapter provides a broad discussion of the two areas that are likely to be of most relevance to the DART project: copyright and breach of confidence.

The main objectives of copyright law are to balance the interests of the creator in their creations with the interests that the public has to access knowledge freely. The *Copyright Act 1968* (Cth) provides a statutory balance which grants exclusive rights to copyright owners and limited fair dealing defences and statutory licences to protect the interests of users. This statutory balance can be altered by contractual arrangements. One of the biggest challenges in managing copyright in an e-Research infrastructure, such as DART, is to establish a legal framework that protects both owners and users of copyright subject matter in ways that do not inhibit the research process.

The concept of the DART project is not only to enable copyright subject matter to be created and stored in depositories but also to provide the tools for this material to be altered and annotated and accessed electronically by a range of people during the research collaboration. This means that copyright subject matter will be in a dynamic state with possibly many different authors who are employed by different institutions. The opportunities for infringement of copyright are extreme.

The legal framework for regulating issues of ownership and distribution of rights in copyright in an e-Research infrastructure will be established primarily by means of contractual arrangements among parties involved in e-Research transactions. It is essential for the owners of copyright subject matter to be identified with accuracy and for them to grant the necessary rights to others who will use the DART infrastructure. The work of both the ARROW and the OAK law projects can inform the development of the necessary legal framework. However, the issues are more complex because DART deals with the entire research process from collection of data, through to storage, annotation and publication. The chapter explores copyright issues

that might arise in some of the specific factual circumstances that may arise at specific stages of the e-Research process.

Protection of confidential information is available through terms in contracts or via the equitable action for breach of confidence. Generally it is the person to whom a duty of confidence is owed who can bring the action for breach of confidence to restrain its unauthorised use or disclosure. The Chapter describes the requirements for a successful action for breach of confidence. It also explores some of the specific factual circumstances that may arise at specific stages of the e-Research process. The equitable action for breach of confidence is invaluable for protecting against unauthorised uses and disclosure of confidential information where there is no contractual relationship between the parties. However, wherever possible, issues of confidentiality should be identified in advance so that a contract can impose the necessary restrictions.

Issues for Discussion

Feedback from DART researchers is requested in relation to the following matters:

Question 3.1

Are there any factual scenarios that you can think of that might give rise to concerns about intellectual property matters which have not been addressed in the Interim Report?

Question 3.2

Should the final report include some commentary on patents for inventions or any of the other forms of IP?

Question 3.3

Will any repository within the DART infrastructure (as distinct from ARROW) act as an 'archive' within the meaning of the *Copyright Act 1968* (Cth)?

Question 3.4

Are there circumstances in which copyright material might be created that are not included within any of the general categories set out in this chapter?

Question 3.5

Would it be helpful to provide a chart that analyses how the DEST funding agreement, the DART agreement and the institutional IP policies and employment contracts deal with ownership of IP?

Question 3.6

Are the descriptions of the various demonstrator models accurate? Is there anything we should add?

Question 3.7

In your view, how realistic are the factual scenarios set out in this chapter? Is there anything that is inaccurate in the descriptions of the project?

Are there any specific factual scenarios that you would like analysed as part of the final report?

Question 3.8

Have there been any important developments in the DART project since the Interim Report was written that are relevant to this chapter?

1.4 PRIVACY AND RELATED LAWS

The main legal issues associated with privacy and related laws are explained in Chapter Five of the *Interim Report*.

Privacy obligations are relevant to the DART project to the extent that it includes identifiable personal information about individuals (including research subjects, researchers and others). Australian and overseas privacy/data protection laws (including health records laws) impose limitations on the collection, use and disclosure of identifiable personal information and also requirements to provide access and amendments rights. They also impose limitations on the transfer of information between different states and countries. The main objectives of information privacy laws are to impose fair information practices in relation to identifiable personal information thereby giving individuals some level of control over their own personal information. Two of the biggest challenges in managing privacy risks (other than security risks which are dealt with in Chapter 8) relate to the uncertainties concerning what constitutes identifiable (and de-identified data) and in managing transborder data flow restrictions in Australian and overseas privacy laws.

The legal frameworks which regulate privacy within Australia are very complex and fragmented. In the context of an e-research environment which spans multiple jurisdictions this makes it important as far as possible to implement procedures which will meet the requirements of all applicable regimes (including public and private sector laws and health records regimes). It is also important to implement procedures to deal with transborder data flow restrictions affecting the flow of personal data across jurisdictional boundaries.

It should not be assumed that aspects of the DART project which do not involved the collection of identifiable personal information about research subjects will not raise privacy issues. The analysis of the demonstrator projects in the Interim Report suggests that such data may be collected incidentally and that projects will in any case involve the collection, use and disclosure of identifiable personal information about researchers. It will therefore be necessary to implement procedures to deal with notification at the time of collection for future data collections and for ensuring that any necessary consents are obtained for any uses and disclosures of other information for purposes other than the original purpose for collection. It will also be necessary to implement procedures for access and amendment and to draft contractual provisions to address transborder data flow issues.

Other related obligations discussed include access and amendment obligations under Freedom of Information laws and curation obligations under archives/public records laws.

Issues for Discussion

Feedback from DART researchers is requested in relation to the following matters:

Question 4.1

Are there any factual scenarios that you can think of that might give rise to concerns about privacy which have not been addressed in the Interim Report?

Question 4.2

Would you like to be provided with more detailed information about specific information privacy principles?

Question 4.3

Is there a need for more detailed information about Health Records laws?

Question 4.4

Do you anticipate any situations in which the use of personal data as part of DART will require amended approvals from Human Ethics Committees?

Question 4.5

Would it be helpful for you to be provided with draft contractual provisions to address transborder dataflow restrictions?

1.5 INFORMATION SECURITY

Chapter Six of the *Interim Report* deals with the legal problems associated with managing information security issues in the DART project.

Information security is vital to the DART project because:

- of the inherent risks associated with information in an on-line environment; and
- the need to manage access to information resources.

Managing the risks associated with information security depends upon a combination of technological measures, policies and procedures, and laws. One of the biggest challenges in managing information security risks in an e-Research infrastructure is establishing an appropriate legal framework for protecting information security.

The legal rules that regulate information security in an e-Research infrastructure, like that envisaged by the DART project, will be established mainly by contractual arrangements among those involved in e-Research transactions, principally the institutions concerned. The contractual arrangements should appropriately assign responsibility for potential losses incurred from information security problems. Before responsibility is allocated, however, it is essential to know precisely what liabilities there might be. The sorts of legal liabilities that could arise depend upon the kinds of information security systems that are adopted.

The information security systems adopted by the DART project include systems based on Public Key Infrastructure (PKI) and federated identity systems. The main sources of legal liability for parties involved in systems such as these potentially include: breaches of information privacy laws; breaches of confidence; breaches of contract; and negligence. The *Interim Report* focuses on liability for negligent acts or omissions, as we think that this will be the most important source of liability in practice.

An action in negligence is available against someone who fails to take reasonable care to avoid foreseeable risks of legally recognised harm to someone else. Unfortunately, there are considerable areas of legal uncertainty concerning the liability of parties involved in e-Research infrastructures for losses arising from negligence. This is especially the case in relation to purely economic losses. Moreover, until now, there has been no published legal analysis of the potential liability of parties involved with

federated identity systems, such as Shibboleth. The main areas of uncertainty are explained in chapter seven of the report.

Specific fact-based examples of the legal liability of participants in e-Research transactions for problems with information security systems, and for losses arising from security breaches, are set out in Appendix 1 to this *Interim Report*. We hope that these examples will prompt you to think further about some of the problems that might arise in practice.

It is extremely important that the identification of the legal issues associated with information security systems is based on an accurate and precise understanding of the systems used in the DART project. We are relying upon DART researchers to identify any omissions or inaccuracies in the discussion of information security systems included in this chapter.

Issues for Discussion

Feedback from DART researchers is requested in relation to the following matters:

Question 5.1

Are the descriptions of the DART information security systems outlined in the Interim Report accurate, complete and up to date?

Question 5.2

Have there been any important developments in the DART security framework since the Interim Report was written?

Question 5.3

In your view, how realistic, and how accurate, are the factual scenarios set out in Appendix 1?

Question 5.4

Are there any additional factual scenarios that you can think of that might create concerns about potential legal liability?

Question 5.5

In your view, who should be responsible for drafting contractual provisions dealing with potential legal liabilities for losses arising from e-Research information security systems?

Question 5.6

Are you are aware of any existing contractual models that might be used or adapted by the DART e-Research infrastructure to deal with potential liability issues?

2 THE DEVELOPMENT OF E-RESEARCH

2.1 INTRODUCTION

The international research landscape is increasingly being shaped by two inter-related developments, an increased commitment on the part of governments and others to the promotion of open access to information, and a new wave of developments in information and communication technologies (ICTs) which have enhanced the information-sharing capabilities of the Internet. An initial series of projects involving the development of institutional repositories for the sharing of published data and other outcomes of research projects has been followed by a second wave of projects that go further and involve the development of the necessary infrastructure for sharing the raw data which forms the basis for research.¹

The new infrastructure projects, which make possible the transfer and sharing of much larger quantities of data than has been possible in the past, have resulted in a paradigm shift to new research methodologies based on sharing and collaboration. In doing so, they have opened up a Pandora's box of policy and legal issues.

This chapter begins by setting out a brief history of the new e-Research movement. This is followed by an overview of the key projects and developments in Europe, North America, Canada and Australia. Finally, a summary of DART and the next phase of the project, known as ARCHER, will be provided along with a discussion of how these projects fit within the new phase of e-Research initiatives.

2.2 THE EVOLUTION OF E-RESEARCH

2.2.1 Background

The new e-Research paradigm must be understood within the broader context of ongoing social and economic trends, and recent initiatives that respond to such trends. The rapid development of ICTs has paved the way for a new social ordering in which information and technology both play a critical role. The concept of an 'Information Society' reflects a growing awareness of the potential for ICTs to contribute to economic, social and educational goals and, consequently, to the importance of ensuring increased access to such technologies for all members of the community. Likewise, the related term 'Knowledge Society' has come to be used to emphasise the fact

that society's most valuable asset is its investment in intangible, social and human capital, where the most important aspects are knowledge and creativity.²

Recognition of the significance of information and knowledge has led to an appreciation of the economic and social importance of access to information. This has recently been seen in the outcomes of the World Summit on the Information Society (WSIS), which was held in two phases over the period 2003-2005.³ At the same time, there has been an increased emphasis on the desirability of public access to publicly funded research.⁴

Associated with, but distinct from, concerns relating to access to publicly funded research, has been a broader movement aimed at promoting greater access to scholarly research and information sources, which may be loosely referred to as the 'open access' movement.⁵ In part, the movement has been motivated by funding constraints facing libraries and academic institutions. The 'open access' movement has also been influenced by concerns amongst academics and others regarding the potential consequences of increasing levels of protection of intellectual property rights. The movement has resulted in initiatives, such as the *Berlin Declaration on Open Access to Knowledge in the Sciences and Humanities*, which has been supported by influential German academic institutions.⁶ The Berlin Declaration, which defines 'open access' as 'a comprehensive source of human knowledge and cultural heritage that has been approved by the scientific community', relies, to an extent, on academic community standards to ensure open access to research resources.

A potentially complementary development has been the establishment of the Creative Commons⁷ and Science Commons⁸ projects. Rather than relying upon academic norms, the Creative Commons and Science Commons initiatives essentially adapt the model pioneered by open source software licensing, whereby intellectual property licensing is used as a means for ensuring open access to material protected by intellectual property. Thus, under the Creative Commons initiatives, a range of standardised copyright licences are used to grant certain rights of use and access to the public while, depending on the licence, particular residual rights are retained by the copyright owners. The potential role of Creative Commons licensing in promoting scholarly research and communication is a fertile area for future research. In Australia, some of this research is being conducted by the OAK (Open Access to Knowledge) Law Project, which is based at Queensland University of Technology (QUT).⁹

2.2.2 Developments involving the Internet and the World Wide Web

In examining the range of current developments, it is important to understand the problems that the various projects aimed at harnessing ICTs for the purposes of research seek to address. Significant weaknesses have been identified in current knowledge management systems in relation to searching for information, extracting information, maintaining information and allowing for automatic document generation.¹⁰ The increased use of metadata and the development of better metadata standards are central elements of those projects aimed at overcoming these deficiencies. Metadata, which literally means 'data about data', is defined in regards to web-design as 'machine understandable information about web resources or other things'.¹¹ It allows users to locate what they specifically require from a mass of information.

The diverse range of policy and legal developments aimed at expediting access to, and use of, research resources referred to above have been paralleled by projects aimed at enhancing the information sharing capabilities of the Internet and World Wide Web. The development of the Internet and the World Wide Web marked an important milestone in the ability of researchers and others to access and share information on a large scale. The convergence of increasingly powerful computers with communications technologies and a common platform for the sharing of information made it theoretically possible to transfer and process large quantities of information at high speed and comparatively low cost. However, the extent and scale of information sharing was initially constrained by limitations in bandwidth and on the ability of individuals to make meaningful use of the plethora of data that was now potentially available. These constraints are gradually being eroded by a complex range of initiatives.

One important set of developments has concerned changes to the way in which the World Wide Web (WWW) is used and the range of applications that it makes available. This has led to the coining of the concept 'Web 2.0'¹² to describe a new web environment characterised by its increased use as a platform for new applications and phenomena such as 'blogs'¹³, 'wikis'¹⁴ and 'tagging'.¹⁵ Web 2.0 is 'often applied to perceived ongoing transition of the WWW from a collection of websites to a full-fledged computing platform serving web applications.'¹⁶ It is commonly understood to refer to developments such as the transition of websites from isolated information silos to sources of content and functionality, a new approach to web content characterised by open communication, decentralisation of authority and freedom to share and re-use.¹⁷

The Semantic Web, a collaborative effort led by the World Wide Web Consortium (W3C),¹⁸ builds on W3C's previous metadata activity and

provides 'an extension of the current web in which information is given well-defined meaning, better enabling computers and people to work in cooperation'.¹⁹ It provides a universal medium for information exchange by giving meaning to the content of documents in a manner that is understandable to machines. In February 2004 the Consortium released two W3C Recommendations: the Resource Description Framework (RDF), which is used to 'represent information and to exchange knowledge in the Web',²⁰ and the Web Ontology Language (OWL), which is used to 'publish and share sets of terms called ontologies, supporting advanced Web search, software agents and knowledge management'.²¹ As stated in the W3C's Semantic Web Activity Statement, the Web will only reach its full potential when 'data can be shared and processed by automated tools as well as by people'.²² An important aspect of the Semantic Web is that it will not only provide metadata about documents stored on the Web, but also about 'things',²³ thereby leading to what is sometimes known as 'the Internet of things'. This transformation of the Web has significant implications for e-Science and the management, access and sharing of information resources generally.

Another important initiative, known as Internet2,²⁴ has as its goal the creation of 'a leading edge network capability for the national research community; enable revolutionary Internet applications; and ensure the rapid transfer of new network services and applications to the broader Internet community'.²⁵ The key feature of the projects associated with the Internet2 consortium is the development of applications and technologies for high-speed data transfer, which may eventually be incorporated in a new high-speed Internet backbone.

2.2.3 Grid computing

The 'grid', or 'cyberinfrastructure' as it is referred to in the US, is an emerging computing model which uses 'the resources of many separate computers connected by a network'²⁶ to obtain higher levels of computational power and data processing. The term 'grid' was chosen to draw an analogy to the electricity power grid, where in this case, data, computational resources and instruments can be regarded as utilities that can be delivered over the network.²⁷ Likewise, the term cyberinfrastructure, draws an analogy with physical infrastructures such as roads and power grids that support modern society.²⁸ The cyberinfrastructure has been defined as 'a system that: coordinates resources that are not subject to centralized control; using standard, open, general-purpose protocols and interfaces; to deliver nontrivial qualities of service'.²⁹

A major aspect of grid computing/cyberinfrastructure has been the development of middleware. Middleware refers to the software services and tools that allow the linkage of information/data resources and computing capability from various sources.³⁰ This is now complemented by the Semantic

Grid, which can be defined as 'an extension of the current Grid in which information and services are given well-defined meaning, better enabling computers and people to work in cooperation.'³¹ As explained on the Semantic Grid Community Portal, this approach is 'essential to achieve the full richness of the Grid vision, with a high degree of easy-to-use and seamless automation enabling flexible collaborations and computations on a global scale.'³² Since the writing of the report, 'Research Agenda for the Semantic Grid: A Future e-Science Infrastructure'³³ in 2001, a series of activities have been established to encourage the development of the Semantic Grid, including the GGF Semantic Grid Research Group and the Semantic Grid Community Portal.³⁴

2.2.4 The New e-Research Projects

An important outcome of the above developments has been the funding by governments and other groups of a range of projects which are designed to harness ICTs and the grid for the purposes of research. These projects were initially focused on improving access to research resources at a systemic level, especially via digital repositories. However, more recently expansions in bandwidth coupled with a growing awareness of potential benefits of sharing expensive scientific equipment has led to an expansion of the concept of sharing to the level of primary research data.

A new breed of research techniques, termed 'e-Research' have arisen, which can be described as 'research activities that use a spectrum of advanced ICT capabilities and embraces new research methodologies.'³⁵ e-Research differs from more traditional research in that it is generally team based and involves collaboration across institutional and jurisdictional boundaries. e-Research also allows users to manage all data and information in a well organised and easily accessible environment.

A major impetus for the new developments has come from the science-based disciplines. Consequently, the term 'e-Science'³⁶ is sometimes used interchangeably with e-Research. As described by the UK National e-Science Centre, 'e-Science will refer to the large scale science that will increasingly be carried out through distributed global collaborations enabled by the Internet. Typically, a feature of such collaborative scientific enterprises is that they will require access to very large data collections, very large scale computing resources and high performance visualisation back to the individual user scientists'.³⁷

As other disciplines are now actively seeking to harness the potential of ICT for their research, the term 'e-Science' has since been augmented by a new term, 'e-Social Science'.³⁸ Once again the main emphasis is on distributed

global collaborations involving large-scale resources and large groups of people.

2.2.5 Key Developments

Governments throughout the world have contributed funding to a number of specific initiatives designed to foster e-Research. These include the projects outlined immediately below, as well as related projects in a number of Asian countries including China, Korea and Japan.³⁹

2.2.6 Europe

Developments in the UK began with the e-Science program, which initially involved an allocation of funding for programs funded by individual Research Councils⁴⁰ and a core e-Science Program developed as a cross-Council activity to develop and broker generic technology solutions and generic middleware to enable e-Science. The first stage of the program was structured around six key elements, including a national e-Science centre, linked to a network of regional grid centres, and the development of generic grid middleware and demonstrator projects. A second phase involves a further six elements including the establishment of the Open Middleware Infrastructure Institute and a Digital Curation Centre.⁴¹

The related e-Social Science program is funded by the Economic and Social Research Council to investigate and promote the use of e-Science to benefit social science research. The majority of the Centre's research is undertaken via seven research nodes, including the Mixed Media Grid and the Oxford e-Social Science project. The latter includes projects which examine the ethical, legal and institutional dynamics of the e-Sciences,⁴² and the manner in which institutional, legal and social settings of scientists may constrain and facilitate e-Science.⁴³ The e-Social Science strategy also includes funding for eleven e-Social Science demonstrator models, a training and awareness program co-funded by the Joint Information Systems Committee (JISC)⁴⁴ and a network of access grid nodes to support collaboration between social science researchers across the UK. JISC also funds other related projects in the UK, including the eBank UK project, and the JISC IE Metadata Schema Registry project.⁴⁵ The Metadata project aims to develop 'a metadata schema registry as a pilot shared service within the JISC Information Environment.'⁴⁶

Another initiative, the Enabling Grids for E-science (EGGE) project, brings together experts from a large number of European countries as well as the United States and Israel. These experts share the common aim of 'building

on recent advances in Grid technology and developing a service Grid infrastructure which is available to scientists 24 hours-a-day'.⁴⁷ Although largely funded by EU funding agencies, the project has a world-wide mission and receives contributions from non EU partners, including the US and Russia.

The project will build on the EU Research Network, GÉANT, which began in November 2000 and GÉANT2, which became operational in December 2001.⁴⁸ It will primarily concentrate on three core areas: building a consistent, robust and secure grid network that will attract additional computing resources; continuously improving and maintaining the middleware necessary to deliver a reliable service to users; and attracting new users from industry and science and ensuring they receive a high standard of training and support.

The EU also funds the OntoGrid project, which is working on producing the technologies and infrastructure for developing services for the Semantic Grid that optimise collaboration activities.⁴⁹

2.2.7 United States

Developments in the United States have largely related to projects funded by the National Science Foundation (NSF), which has identified advanced cyberinfrastructure as a major funding priority. The stated aim of its funding is 'to provide user-friendly, reliable information technology and knowledge management resources to all researchers and educators to catalyze discovery at the frontiers of all science and engineering disciplines'.⁵⁰ The NSF's 2006 investments include support for: high-end computing architecture research; preparation of scientists and engineers to effectively use cyberinfrastructure; the Protein Data Bank; the National Radio Astronomy and National Optical Astronomy Observatories;⁵¹ the National STEM Education Digital Library⁵² and Digital Library for Earth Science Education; and social and behavioral science data collections. Support will also be provided to: address issues such as confidentiality protection and means for securing worldwide, user-friendly access; multiple projects to provide the nation's science and engineering community access to high-end computing and other cyberinfrastructure resources; as well as to develop next-generation data management systems and associated tools.⁵³

Projects funded by the NSF as part of this initiative include Privacy, Obligations and Rights in Technologies of Information Assessment (PORTIA), a 'five-year, multi-institutional, multi-disciplinary, multi-modal investigation that looks comprehensively at sensitive data in a networked world'.⁵⁴ The

project focuses specifically on the technical challenges of handling sensitive data and the policy and legal issues facing data subjects, owners and users.

These developments have been supplemented by the activities of EDUCAUSE, a non profit organisation with a mission to advance higher education by promoting the intelligent use of information technology. EDUCAUSE is actively involved in cybersecurity through the EDUCAUSE/Internet2 Computer and Network Security Task Force. Its activities also encompass information systems and services, information technology management and leadership, networking and emerging technologies as well as legal and policy issues.⁵⁵

2.2.8 Canada

The Canadian government has committed CA\$110 million to the establishment of CANARIE's CA*net4, which supersedes CA*net3, a system that was established under its 'Connecting Canada' agenda. CA*net4 is 'a new generation of Internet broadband network architecture that will link all research institutions, including many community colleges, via provincial networks.'⁵⁶

Other projects that are focused upon developing a global communication system for research include Grid Canada, a partnership between CANARIE, the National Research Council (NRC) and C3.ca Association Inc. that aims to 'help enable computers, storage, networks, instruments, and visualization resources to take part in a national grid and make them available to research communities across Canada'.⁵⁷

Further work includes a network of institutional repositories located at 26 university research libraries that are linked through regional initiatives, such as the Ontario Scholars Portal.⁵⁸ The NRC's Canada Institute for Scientific and Technical Information (CISTI) also provides a national repository in all areas of science, technology, engineering and medicine.⁵⁹ Resources available include books, journal articles, conference papers and reports. An evolving system that dates back well into last century, the repository provides access through NRC Information Centres (NICs) located throughout Canada as well as via the Internet. Finally, a non-profit service called Érudit, funded by the Quebec government through the Fonds québécois de recherche sur la société et la culture (Quebec fund for research on society and culture) and Le Fonds de l'autoroute de l'information (information superhighway fund), provides digital versions of academic journals and books.⁶⁰

2.2.9 Australia

In the case of Australia, the recently appointed e-Research Coordinating Committee released an Interim report⁶¹ outlining e-Research issues of national importance in the short and medium term, and associated strategies to address them. Key strategic directions outlined include the linkage of e-Research resources. The report stresses the need for Australia to develop a world-class e-Research capability across all research disciplines. It also points out that facilities which can develop and customise access frameworks, user interfaces, shared services, common use facilities, data curation, user authentication and security services would greatly benefit the Australian e-Research effort.

The Department of Education, Science and Training (DEST) recently released a Strategic Roadmap which outlines the key principles of the newly developed National Collaborative Research Infrastructure Strategy (NCRIS).⁶² The NCRIS is a major initiative under the Australian Government's *Backing Australia's Ability - Building our Future through Science and Innovation*. The aim of NCRIS is to 'bring greater strategic direction and coordination to national research infrastructure investments.' Funding of AU\$542 million to 2011 will be available for researchers to obtain access to major research facilities and supporting networks and infrastructure.

When Backing Australia's Ability was first announced in 2001, the Government stated that they would allocate \$246 million over five years 'to upgrade the basic infrastructure of universities' and to facilitate research.⁶³ Part of this funding has been provided via a Systemic Infrastructure Initiative (SII)⁶⁴ to address the need for accessible data and information repositories, accessible research facilities and instruments, accessible sensor networks, agreed standards for ICT and coordinated development of middleware.

In 2003, funding was given under the SII to four projects, known as the Federated Repositories of Online Digital Objects (FRODO) projects, which were designed to improve the resources available to Australian researchers at a systemic level. FRODO includes projects that aim to: develop software that will create 'better linkages between university information technology systems; 'redevelop the existing central repository of the Australian Digital Theses Program (ADT) to increase its coverage and utility'; and to increase the accessibility and sustainability of digital collections.⁶⁵ A fourth project, The Australian Research Repositories Online to the World (ARROW), led by Monash University, is working on identifying, testing and developing 'software solutions to demonstrate best practice solutions for storing and organising digital information.'⁶⁶ This project focuses upon the deposit of, and

access to, published articles. It will not consider the wider research process of the storage of datasets and using them to produce dynamic publications.

Funding was provided under the SII to nine further projects in 2005, which are collectively known as the Managed Environments for Research Repository Infrastructure (MERRI) projects. A common feature of the MERRI projects is that they are designed to enhance the ability of Australian researchers to tap into new resources and to better share their results with the wider research community. The first group is concerned with the management and integration of large data sets. This group comprises projects that aim to: develop best practice 'principles for data security and sustainability of time critical data'; 'provide a highly distributed archiving facility to support ... long term data curation requirements'; and provide for the linkage and mapping of tissue banks, records, clinical data, images and genetic data across common diseases. A second group focuses on technical development and deployment and comprises projects that will: 'provide a national focal point for advice on open source software for research effectiveness'; 'build a strategic plan of activities and projects for an Australian collaborative middleware strategy'; and 'develop a set of legal protocols and generic licences that can be used across universities to facilitate and break down barriers to open access to copyright material'. The third and final group focuses on interoperability and access.⁶⁷ This group includes the DART project, which will build upon the work completed in the ARROW project, as well as on many other national and international projects.

2.3 THE DART PROJECT

The DART project, which has been funded by DEST under the SII, is designed to create a platform to enable the secure sharing of digital research resources via a research infrastructure that spans universities, including across regional and smaller universities. It essentially sets out to develop a new system for managing research activity and communication, which will address issues that arise throughout the entire research process. In doing so, it aims to support and allow researchers, end users and computer systems to manage the creation, collection, annotation and publication of digital data and documents, whilst increasing access for researchers and the public. Its ultimate objective is to provide greater visibility of and access to publicly funded research.⁶⁸ The project builds on earlier models, such as ARROW, that focus on the storage of existing digital information, by extending the e-Research paradigm to earlier stages of the research process and by increasing the functionality of research tools, including providing tools for annotating research outputs. Significantly, DART aims to provide access to datasets and other digital objects in addition to publications that utilise those datasets. In other words, it aims to enable datasets to be treated in the

same way as are digital publications. The benefits include the prevention of data loss and the ability for researchers to locate archival datasets.⁶⁹

In order to address each area of the e-Research process, the DART project consists of a number of work package groups which reflect the stages of the research process.⁷⁰ The project encompasses three demonstrator models designed to demonstrate how the tools developed under the project can be used in practice by e-Researchers. In this sense, the DART project will provide 'proof of concept' tools that will need to be made suitable for use in the future. The DART project, including the demonstrator models, is discussed in further detail in the next two chapters.

2.4 THE NEXT STAGE: THE ARCHER PROJECT

The DART project is one component of a range of government-funded initiatives that are building Australia's e-Research infrastructure. Essentially, DART is a 'proof of concept', which has investigated the development of new generation research tools. The work undertaken in the DART project will be continued by a new project, known as the Australian ResearCH Enabling enviRonment ('ARCHER'), which will build on work conducted in both the DART and ARROW projects. As with the DART project, the lead institution for ARCHER is Monash University, with James Cook University and the University of Queensland as partner institutions.

ARCHER is one of six new DEST funded projects. In July of this year, DEST announced that it will allocate \$15 million under the SII to six new initiatives. The six projects, which also include ARROW – Stage 2, aim to provide researchers with research infrastructure that will facilitate collaboration both within Australia and overseas.⁷¹

The ARCHER project will enhance research infrastructure and collaboration by developing what is known as 'MyResearchSpace', which is 'an integrated solution' for those involved in e-Research.⁷² Similarly to DART, the ARCHER project will address all stages of the e-Research process. The research stages dealt with by ARCHER are:

- *Conceive* - this stage refers to the period when the researcher or research team forms their original idea. This may involve reviewing experimental results, conducting literature reviews and/or discussions with peers. For this phase of the research process, ARCHER will provide a web-based collaboration space that will integrate information resources, discussions and collaborative documents. ARCHER will also

offer a limited instant messaging and presence-awareness system that will allow real-time collaborations. Furthermore, it will also provide search services across local, national and international repositories.

- *Design* – this stage refers to the period when the design of the research is refined and the experiment, or method of data collection, is planned. The web-based space from the Conceive phase will be made available to users so that they may collaborate while designing their research.

- *Research* – this stage refers to the period when the research is actually conducted. It is the main focus area for ARCHER. The ARCHER project will develop tools in relation to all of the sub-stages of the Research stage, namely the data collection, storage, and data analysis and visualisation stages.
 - 1.1 For the *data collection stage*, ARCHER will support small (sensors), medium (desktop instruments) and large (national major facilities) instruments. ARCHER will allow users to monitor and control instruments remotely. Users will also be able to view data and samples collected in real-time. Those in disciplines that have pre-existing datasets will be able to utilise ARCHER tools to upload their data into a 'collaboration-enabled' data store. In addition, ARCHER will automatically collect metadata where possible for data discovery, reuse and to repeat results.
 - 1.2 In relation to the *storage stage*, ARCHER will use a number of object storage technologies, including Storage Resource Broker (SRB). Furthermore, ARCHER will establish 'YourSRB', which will allow the offline storage of fieldwork and peer-to-peer data management. At the same time, it should be noted that ARCHER will not be an article/eprints publication repository.
 - 1.3 For the *data analysis and visualisation stage*, ARCHER will 'convert' or 'wrap' particular existing analysis code⁷³ so that it can be used within the ARCHER infrastructure. Limited collaborative annotation tools will also be made available that will allow users to comment on data during the *Research* stage.

- *Write* – the writing stage refers to the period when researchers write up their research for journals or conferences. Those that use ARCHER tools will be able to use the collaborative document space, the access to resources, results and blogs, as well as the collaboration annotation tools to assist them in writing about their work.

- *Publish* – the publish stage refers to the period when researchers publish their data. ARCHER will assist users with publishing their data by providing an interface that will allow data to be moved from a collaborative space to a public space. For example, a user may wish to move their data and related metadata into a public repository such as the Protein Data Bank.
- *Expose* – finally, this stage refers to the period when published data needs to be exposed in a controlled manner. ARCHER will provide users with search and discovery tools to allow the discovery of data, annotations and publications stored in repositories.

The tools developed under the ARCHER project will be predominantly available via a Web-based portal,⁷⁴ which will provide research groups with different functionalities. The project will also provide users with web-services interfaces for certain standardised services components that researchers will be able to integrate into their existing data management systems or workflows. The components for ARCHER will support single-sign on ('SSO') to resources and information across institutions.

ARCHER will provide the tools developed as part of the project to research groups represented under the nine high priority capability areas under NCRIS. The nine areas are:⁷⁵

- Integrated biological systems;
- Evolving biomolecular platforms and informatics;
- Characterisation;
- Biotechnology products;
- Fabrication;
- Networked biosecurity framework;
- Integrated marine observing system;
- Optical and radio astronomy; and
- Structure and evolution of the Australian continent.

Moreover, ARCHER will further consider the information management requirements in the Behavioural, Social and Economic Sciences, as well as in the Creative Arts and Humanities.

2.5 SUMMARY

Projects taking place in Europe, US, Canada and Australia are contributing to an important new series of projects that are harnessing modern ICT to promote increased access to and use of research resources, including primary research data. These projects are heralding a new era for research, which is becoming increasingly international, collaborative and interdisciplinary in nature. The DART project is significant to this new movement as it takes a 'whole process' approach to new e-Research environments which encompasses information processing, exchange, utilisation, and management. Various tools developed under the DART project will also be used in the new e-Research initiative, ARCHER, which will provide researchers from a number of disciplines with production-ready software and architecture.

ENDNOTES

¹ This chapter is based upon an article that has been accepted for publication by Online Information Review: Moira Paterson, David Lindsay, Ann Monotti, Anne Chin, 'DART: A new missile in Australia's e-research strategy'.

² European Commission, *Knowledge Society – Homepage* (2006)

<http://europa.eu.int/comm/employment_social/knowledge_society/index_en.htm>.

³ World Summit on the Information Society: World Summit on the Information Society, *Geneva Declaration of Principles*, principles A2 and A7, Document WSIS-03/GENEVA/DOC/4-E (2003) <<http://www.itu.int/wsis/docs/geneva/official/dop.html>>; World Summit on the Information Society, *Tunis Commitment*, principles 9 and 10, Document: WSIS-05/TUNIS/DOC/7- 18 November 2005 (2005) <<http://www.itu.int/wsis/docs2/tunis/off/7.html>>. The 'Geneva Declaration of Principles' affirmed a commitment to build a 'people-centred, inclusive and development-oriented Information Society, where everyone can create, access, utilize and share information and knowledge', while the 'Tunis Commitment' recognised that 'access to information and sharing and creation of knowledge contributes significantly to strengthening economic, social and cultural development'.

-
- ⁴ For example, one of the outcomes of the ministerial meeting of the OECD Committee for Scientific and Technological Policy held in November 2004 was the establishment of an OECD working committee to develop a set of Principles and Guidelines on Access to Research Data from Public Funding: Organisation for Economic Co-operation and Development Newsroom, *Science, Technology and Innovation for the 21st Century. Meeting of the OECD Committee for Scientific and Technological Policy at Ministerial Level, 29-30 January 2004 - Final Communiqué* (2004) <http://www.oecd.org/document/0,2340,en_2649_34487_25998799_1_1_1_1,00.html>; Department of Education, Science and Training e-Research Coordinating Committee, *An E-Research Strategic Framework, A Discussion Paper* (2005) <http://www.dest.gov.au/sectors/research_sector/policies_issues_reviews/key_issues/e_research_consult/discussion_paper.htm>.
- ⁵ Brian Fitzgerald et al, *Oak Law Report* (2006) [1.18]-[1.19] <<http://www.oaklaw.qut.edu.au>>.
- ⁶ E Hoorn, 'Repositories, Copyright and Creative Commons for Scholarly Communication' (2005) 45 *Ariadne* <<http://www.ariadne.sc.uk/issue45/hoorn/>>; Max Planck Society, *Conference on Open Access to Knowledge in the Sciences and Humanities* (2006) <<http://www.zim.mpg.de/openaccess-berlin/berlindeclaration.html>>.
- ⁷ Creative Commons, *Learn More about Creative Commons* (2006) <<http://creativecommons.org/learnmore>>.
- ⁸ Science Commons, *Science Commons* (2006) <<http://sciencecommons.org/>>.
- ⁹ Brian Fitzgerald et al, *Oak Law Report* (2006) <<http://www.oaklaw.qut.edu.au>>.
- ¹⁰ D Fensel, J A Hendler, H Lieberman and W Wahlster 'Introduction' in D Fensel, J A Hendler, H Lieberman and W Wahlster (eds), *Spinning the Semantic Web* (2003) 4.
- ¹¹ T Berners-Lee, *Metadata Architecture* (1997) <<http://www.w3.org/DesignIssues/Metadata.html>>.
- ¹² 'Web 2.0' had its origins in a 2004 conference titled 'Web2.0': T O'Reilly, 'What Is Web 2.0?: Design Patterns and Business Models for the Next Generation of Software' (2005) <<http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html>>.
- ¹³ 'Blog' is short for Weblog, a Web-based journal 'that is frequently updated and intended for general public consumption: bytown internet, *Glossary* (2006) <www.bytowninternet.com/glossary>.
- ¹⁴ A 'Wiki' is 'a type of Website' that allows users to add and edit content easily and is especially suited for collaborative writing: Wikipedia, *Wiki*, (2006) <<http://en.wikipedia.org/wiki/Wiki>>.
- ¹⁵ This involves the use of a metatag – html code used to 'provide a description and to provide keywords for a webpage': Wikipedia, *Meta element* (2006) <http://en.wikipedia.org/wiki/Meta_tag>.
- ¹⁶ Wikipedia, *Web 2.0* (2006) <<http://en.wikipedia.org/wiki/Web2.0>>.
- ¹⁷ Wikipedia, *Web 2.0* (2006) <<http://en.wikipedia.org/wiki/Web2.0>>.
- ¹⁸ The W3C is an international consortium of companies which has the purpose of developing open standards for the web. Information about W3C can be found at: World Wide Web Consortium: World Wide Web Consortium, *About the World Wide Web Consortium (W3C)* (2006) <<http://www.w3.org/Consortium/>>.
- ¹⁹ T Berners-Lee, J Hendler and O Lassila, 'The Semantic Web' (2001) 284 *Scientific American* 34-43.
- ²⁰ World Wide Web Consortium, *Semantic Web* (2006) <<http://www.w3.org/2001/sw/>>.

-
- ²¹ World Wide Web Consortium, *Semantic Web* (2006) <<http://www.w3.org/2001/sw/>>.
- ²² World Wide Web Consortium, *Semantic Web Activity Statement* (2006) <<http://www.w3.org/2001/sw/Activity>>.
- ²³ T Berners-Lee, *Metadata Architecture* (1997) <<http://www.w3.org/DesignIssues/Metadata.html>>.
- ²⁴ Internet2 is a non-profit consortium that was first established in 1997. The term Internet2 properly refers to the consortium itself - which is led by 207 U.S. universities together with private sector partners, including Cisco Systems, Proulx Science and Sun Microsystems – and not to any particular technologies: Internet2®, *About Internet2®* (2006) <<http://www.internet2.edu/about/>>.
- ²⁵ Internet2®, *About Internet2®* (2006) <<http://www.internet2.edu/about/>>.
- ²⁶ Answers.com™, *Grid Computing – wikipedia definition* (2006) <http://www.answers.com/main/ntquery?method=4&dsid=2222&dekey=Grid+computing&gwp=8&curtab=2222_1&linktext=Grid%20Computing>.
- ²⁷ P Hobson (2004), 'From Computing to the Power Grid' (2004) 20 *Frontiers* <<http://www.pparc.ac.uk/frontiers/archiveText/update.asp?id=20U6&style=update>>.
- ²⁸ D Hart, 'National Science Foundation Releases New Report from Blue-Ribbon Advisory Panel on Cyberinfrastructure' (2003) *NSCA News* <http://access.ncsa.uiuc.edu/Releases/03Releases/02.03.03_National_S.html>.
- ²⁹ Ian Foster, 'What is the Grid? A Three Point Checklist' (2002) 1 No. 6 *Grid Today* <<http://www.gridtoday.com/02/0722/100136.html>>.
- ³⁰ Department of Education, Science and Training, e-Research Coordinating Committee, *An E-Research Strategic Framework, Discussion Paper* (2005) 14 <http://www.dest.gov.au/sectors/research_sector/policies_issues_reviews/key_issues/e_research_consult/discussion_paper.htm>.
- ³¹ Semantic Grid, *Semantic Grid Community Portal* (2006) <<http://www.semanticgrid.org/>>.
- ³² Semantic Grid, *Semantic Grid Community Portal* (2006) <<http://www.semanticgrid.org/>>.
- ³³ D De Roure, N Jennings and N Shadbolt, 'Research Agenda for the Semantic Grid: A Future e-Science Infrastructure', Technical report UKeS-2002-02, UK e-Science Technical Report Series, National e-Science Centre (2001).
- ³⁴ Semantic Grid, *Semantic Grid Community Portal* (2006) <<http://www.semanticgrid.org/>>.
- ³⁵ Department of Education, Science and Training, *e-Research* (2005) <http://www.dest.gov.au/sectors/research_sector/policies_issues_reviews/key_issues/e_research_consult/default.htm>.
- ³⁶ 'E-science' refers to 'science that is enabled by the routine use of distributed computing resources by end-user scientists': Geoffrey Fox and David Walker, *e-Science Gap Analysis* (2003) <<http://www.grid2002.org/ukescience/gapresources/GapAnalysis30June03.pdf>>; UK e-Science Program, *escience-grid.org.uk* (2006) <http://www.escience-grid.org.uk/>; CCLRC e-Science Centre, *home* (2006) <<http://www.e-science.clrc.ac.uk>>; National e-Science Centre, *Defining e-Science* (2006) <<http://www.nesc.ac.uk/nesc/define.html>>.
- ³⁷ National e-Science Centre, *Defining e-Science* (2006) <<http://www.nesc.ac.uk/nesc/define.html>>.

-
- ³⁸ 'e-Social Science' has been defined as 'social science using grid computing': Answers.com™, *E-Social Science* (2006) <<http://www.answers.com/topic/e-social-science-1?hl=social&hl=science>>.
- ³⁹ These projects are summarised in: Department of Education, Science and Training e-Research Coordinating Committee, *An E-Research Strategic Framework, A Discussion Paper* (2005) Appendix C <http://www.dest.gov.au/sectors/research_sector/policies_issues_reviews/key_issues/e_research_consult/discussion_paper.htm>.
- ⁴⁰ The Councils were created to fulfil the objectives set out in: UK Government, *Realising our potential: a Strategy for Science, Engineering and Technology* (1993). The Councils are controlled by the Department of Trade and Industry: Research Councils UK, *Home* (2005) <<http://www.rcuk.ac.uk/about.asp>>.
- ⁴¹ Research Councils UK, *About the UK e-Science Programme* (2004) <<http://www.rcuk.ac.uk/escience/>>.
- ⁴² Oxford Internet Institute, *e-Science* (2006) <<http://www.oii.ox.ac.uk/research/?rq=escience>>.
- ⁴³ Oxford Internet Institute, *e-Science* (2006) <<http://www.oii.ox.ac.uk/research/?rq=escience>>.
- ⁴⁴ The Joint Information Systems Committee is funded by the UK Further and Higher Education Funding Councils, and provides 'strategic guidance, advice and opportunities to use ICT to support teaching, learning, research and administration' in the tertiary education sector: Joint Information Systems Committee, *About JISC* (2006) <<http://www.jisc.ac.uk/index.cfm?name=about>>.
- ⁴⁵ Information on the JISC Information Environment can be accessed at: Joint Information Systems Committee, *Information Environment* (2006) <http://www.jisc.ac.uk/index.cfm?name=ie_home>.
- ⁴⁶ JISC IE Metadata Schema Registry, *Home* (2006) <<http://www.ukoln.ac.uk/projects/iemsr/>>.
- ⁴⁷ EGEE, *Welcome to EGEE* (2006) <<http://public.eu-egee.org/>>.
- ⁴⁸ GÉANT, *Welcome to the GÉANT Website* (2005) <<http://www.geant.net/>>; GÉANT2, *Welcome to the GÉANT2 Website* (2006) <<http://www.geant2.net/>>.
- ⁴⁹ OntoGrid Project, *Home* (2006) <<http://www.ontogrid.net/ontogrid/index.jsp>>.
- ⁵⁰ National Science Foundation (2005), *NSF-wide investment – Cyberinfrastructure* <http://www.nsf.gov/news/priority_areas/cyberinfrastructure/index.jsp>.
- ⁵¹ National Science Foundation, *National Optical Astronomy Observatory (NOAO)* (2006) <http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=5663>; National Science Foundation, *National Radio Astronomy Observatory (NRAO)* (2006) <http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=5653&org=AST&from=home>.
- ⁵² National Science Foundation, *National STEM Education Digital Library (NSDL)* (2005) <<http://www.nsf.gov/ehr/rec/nsdllinks.jsp>>.
- ⁵³ National Science Foundation (2005), *NSF-wide investment – Cyberinfrastructure* <http://www.nsf.gov/news/priority_areas/cyberinfrastructure/index.jsp>.
- ⁵⁴ Privacy, Obligations, and Rights in Technologies of Information Assessment, *Project Description* (2006) <<http://crypto.stanford.edu/portia/>>.
- ⁵⁵ EDUCAUSE, *What is EDUCAUSE?* (2006) <http://www.educause.edu/content.asp?PAGE_ID=720&bhcp=1>.

-
- ⁵⁶ Government of Canada, *Achieving Excellence: Investing in People, Knowledge and Opportunity* (2002) Section 3 Government Support for Innovation – 1995-2001- Canada's Innovation Strategy <<http://www.innovationstrategy.gc.ca/gol/innovation/site.nsf/en/in04158.html>>.
- ⁵⁷ Grid Canada, *About GC* (2002) <<http://www.gridcanada.ca/about.html>>. 'Visual resources' in technological terms are services that assist users with the visualisation of messages or data. Information visualisation involves computer programs transforming and representing abstract data in a manner that enhances human understanding: Wikipedia, *Visualization (graphic)* (2006) <http://en.wikipedia.org/wiki/Visualization_%28graphic%29>.
- ⁵⁸ Scholars Portal, *Welcome to Scholars Portal* (2005) <<http://www.scholarsportal.info/>>.
- ⁵⁹ Canadian Institute for Scientific and Technical Information, *Welcome* (2006) <http://cisti-icist.nrc-cnrc.gc.ca/cisti_e.html>.
- ⁶⁰ Érudit, *Journals* (2006) <<http://www.erudit.org/en/revue/index.html>>.
- ⁶¹ Department of Education, Science and Training e-Research Coordinating Committee, *An E-Research Strategic Framework, Discussion Paper* (2005) <http://www.dest.gov.au/sectors/research_sector/policies_issues_reviews/key_issues/e_research_consult/discussion_paper.htm (accessed 21 March 2006)>.
- ⁶² Department of Education, Science and Training, *National Collaborative Research Infrastructure Strategy, Strategic Roadmap* (2006) <http://www.dest.gov.au/sectors/research_sector/policies_issues_reviews/key_issues/ncris/>.
- ⁶³ Department of Education, Science and Training, *Systemic Infrastructure Initiative (SII)* (2005) <http://www.dest.gov.au/sectors/higher_education/programmes_funding/programme_categories/research_related_opportunities/systemic_infrastructure_initiative/>.
- ⁶⁴ See the following for a list of SII projects funded up until 2006: Department of Education, Science and Training, *Systemic Infrastructure Initiative - Funded Projects* (2005) <http://www.dest.gov.au/sectors/higher_education/programmes_funding/programme_categories/research_related_opportunities/systemic_infrastructure_initiative/sii_funded_projects.htm>.
- ⁶⁵ Department of Education, Science and Training, *ARIIC Projects* (2005) <http://www.dest.gov.au/sectors/research_sector/policies_issues_reviews/key_issues/australian_research_information_infrastructure_committee/ariic_projects.htm>.
- ⁶⁶ Department of Education, Science and Training, *ARIIC Projects* (2005) <http://www.dest.gov.au/sectors/research_sector/policies_issues_reviews/key_issues/australian_research_information_infrastructure_committee/ariic_projects.htm>.
- ⁶⁷ For details on the MERRI project, see: Department of Education, Science and Training, *ARIIC Projects* (2005) <http://www.dest.gov.au/sectors/research_sector/policies_issues_reviews/key_issues/australian_research_information_infrastructure_committee/ariic_projects.htm>.
- ⁶⁸ DART, *DART Bid Document (public version)* (2005) 2-3 <http://www.dart.edu.au/DART_Bid_Document.pdf>. See also: Andrew Treloar, *The Dataset Acquisition, Accessibility, and Annotation e-Research Technologies (DART) Project: building the new collaborative e-research infrastructure* (2006) <<http://ausweb.scu.edu.au/aw06/papers/refereed/treloar/paper.html>>.
- ⁶⁹ DART, *DART Bid Document (public version)* (2005) 3, 11 <http://www.dart.edu.au/DART_Bid_Document.pdf>. See also: Andrew Treloar, *The Dataset Acquisition, Accessibility, and Annotation e-Research Technologies (DART) Project: building the*

new collaborative e-research infrastructure (2006)

<<http://ausweb.scu.edu.au/aw06/papers/refereed/treloar/paper.html>>.

⁷⁰ The DART work packages are outlined in: DART, *DART Bid Document (public version)* (2005) Appendix A <http://www.dart.edu.au/DART_Bid_Document.pdf>.

⁷¹ The Hon Julie Bishop MP, *Media Centre* (2006)

<<http://www.dest.gov.au/Ministers/Media/Bishop/2006/07/B001310706.asp>>.

⁷² ARCHER: *Functionality Overview for Researchers, or, What ARCHER provides and why you should be interested*, page 1.

⁷³ Analysis codes are computer programs that can be used to analyse data. Analysis code is widely used in science to undertake calculations for research. For examples, see: Greg Sjaardema, *Sandia Engineering Analysis Code Access System (SEACAS)* (1998)

<<http://endo.sandia.gov/SEACAS/Documentation/SEACAS.html>>; TOPDAC, *home page* (2000)

<<http://w3.pppl.gov/topdac/>>.

⁷⁴ A 'Web portal', or 'portal' is a Web site or service that provides a variety of services and resources, such as search engines and email: Wikipedia, *Web portal* (2006)

<http://en.wikipedia.org/wiki/Web_portal>.

⁷⁵ National Collaborative Research Infrastructure Strategy (NCRIS), *Investment Framework* (2006) 4 <<http://www.ncris.dest.gov.au/NR/rdonlyres/ABBD6B83-E314-4237-9A75-7D48E35FC92C/10176/NCRISInvestmentFrameworkapprovedbyMinisterBishopAp.pdf>>.

3 THE DART PROJECT

3.1 INTRODUCTION

The DART project aims to provide tools and services for researchers across the entire e-Research process, from the creation and collection of raw data, to the publication of research outcomes.

This chapter provides an outline of the structure of the DART project and how the project will enhance the e-Research process. It also provides a brief summary of the tasks and specific goals allocated to each of the work package groups established under the DART project.

The structure and benefits of the DART project

The DART project has been structured around the following five stages of the e-Research process, namely:

- Data collection;
- Data storage;
- Data analysis and annotation;
- Publication of research; and
- Discovery and access to data and publications.

As shown in Figure 3.1 below, the project will provide a system that deals with large-scale data collection from various sources and the storage of this data in repositories. Researchers will be able to use DART to store a variety of digital objects, including raw data from instruments. The project will also allow collaborative research groups, as well as individual researchers, to analyse, annotate and publish stored data. Researchers and other users will be able to access data stored in repositories via the use of appropriate access tools.

Figure 3.2 below illustrates the current circumstances for each step in the scholarly process and how they will be altered by the DART project. It also outlines the benefits for researchers and the general public.

Figure 3.1 - DART project high level architecture¹



Figure 3.2 - How the DART project will enhance the e-Research process²

Scholarly Processes	Research	Registration	Certification	Awareness	Archiving	Annotation	Rewarding
Process Outputs							
Current issues	<ul style="list-style-type: none"> Poor curation Fragmented collaboration Poor support for sensors, large datasets 	<ul style="list-style-type: none"> Reliant on journal processes Rarely possible for datasets 	<ul style="list-style-type: none"> Based on journal quality as proxy for article Datasets problematic 	<ul style="list-style-type: none"> Hard to discover datasets and other digital objects 	<ul style="list-style-type: none"> Reliant on journals Poor support for datasets 	<ul style="list-style-type: none"> No ability for annotation of publications or datasets 	<ul style="list-style-type: none"> Largely based on publications Based on peer evaluations
DART will provide support for	<ul style="list-style-type: none"> Data curation Collaboration support Support for eResearch 	<ul style="list-style-type: none"> Immediate registration Datasets and other digital objects accepted 	<ul style="list-style-type: none"> Other quality measures possible Digital objects rateable 	<ul style="list-style-type: none"> Datasets now treated in same way as publications 	<ul style="list-style-type: none"> Datasets now treated in same way as publications Secure archive 	<ul style="list-style-type: none"> Annotation of publications or datasets by researchers and readers 	<ul style="list-style-type: none"> Now based on datasets and annotations Visible to wider group
DART Benefits for Researchers	<ul style="list-style-type: none"> More effective research No data loss 	<ul style="list-style-type: none"> Guaranteed priority Range of digital objects 	<ul style="list-style-type: none"> Better assessment of all research outputs 	<ul style="list-style-type: none"> Easier to locate and build on existing work 	<ul style="list-style-type: none"> Ability to locate archival datasets No data loss 	<ul style="list-style-type: none"> Improved collaboration and validation Faster communication 	<ul style="list-style-type: none"> More immediate feedback
DART Benefits for Public	<ul style="list-style-type: none"> Better use of taxpayer funds Improved research research outcomes 	<ul style="list-style-type: none"> Improved efficiency Visibility of priority claims 	<ul style="list-style-type: none"> Better visibility of quality measures for range of outputs 	<ul style="list-style-type: none"> More efficient research Improved research outcomes 	<ul style="list-style-type: none"> Access to archived data Improved visibility over research outputs 	<ul style="list-style-type: none"> Visibility into research process Ability to annotate! 	<ul style="list-style-type: none"> Ability to influence rewards Improved research outcomes

3.2 THE DART PROJECT WORK PACKAGE GROUPS

There are five categories of DART project work packages which each reflect a stage of the e-Research process.

Data Collection, Monitoring and Quality Assurance (DMQ)

The DMQ work packages investigate issues concerning the collection, monitoring and quality of large data streams.

Common Instrument Middleware Architecture (CIMA): an architecture developed by the CIMA group, based at Indiana University, which allows instrument and sensor connection to the Internet, while making data discoverable and results publishable using open grid services architecture or web services.³

JCU and Indiana Instrument Services package (JAINIS): a middleware package based on CIMA being developed by James Cook University.

Storage Resource Broker (SRB): a client-server middleware that provides a uniform interface for connecting to heterogeneous data resources over a network and accessing replicated data sets. SRB, in conjunction with the Metadata Catalog (MCAT), provides a way to access data sets and resources based on their attributes and/or logical names rather than their physical locations or names.⁴

These packages address the requirements involved in dealing with large datasets, including streams created at a high rate via the linkage of instruments and sensors to remote users and collection facilities. DART has been collaborating with the CIMA group at Indiana University.

The DART crystallography demonstrator project, which is discussed in Chapter 5, predominantly uses CIMA to put a number of X-ray instruments on-line. It will use the JAINIS package to acquire and package streaming crystallography data from instruments.

The specific objectives of the DMQ work packages are as follows:⁵

- DMQ1: to connect instruments and sensors to the DART network by establishing and implementing a security policy framework;

- DMQ2: using SRB, to connect selected instruments and sensors to storage repositories through CIMA middleware;
- DMQ3: to ensure that data obtained from instruments and sensors is of sufficient quality to warrant curation. To check the calibration of sensors and instruments and validate instruments and data;
- DMQ4: to allow online, remote access to sensors and instruments involved in pilot projects; and
- DMQ5: to enhance the intelligence of the storage framework by building event triggers into the SRB.

3.2.1 Storage and Interoperability (SI)

The SI work packages focus on the security and accessibility of a range of digital objects, including datasets, documents, software, simulations, and dynamic knowledge representations. The SI work packages consider the collection of data from devices, the security of data during transfer between networks, the storage of data on high-capacity devices, the preservation and management of data in repositories and ensuring the integrity of data.

Fedora: Fedora is 'open source software that gives organisations flexible tools for managing and delivering their digital content.'⁶

The specific objectives of the SI work package group are as follows:

- SI1: to facilitate distributed data management by integrating SRB, as the underlying data grid, into the repository software Fedora;
- SI2: to enhance interoperability between SRB based environments and Fedora, thereby allowing interoperability between repositories not based on Fedora and existing institutional repositories;
- SI3: to improve discovery by fostering richer descriptive and preservation metadata for dataset objects;
- SI4: to utilise Grid security to establish a secure service for transferring data from sensors and instruments to repositories;
- SI5: to create an abstraction layer that supports a variety of data replication systems,⁷ thereby allowing access to data regardless of the underlying replica system that is utilised;
- SI6: to provide a software implementation that allows data to be retrieved from repositories or regenerated dynamically using standard metadata;⁸

- SI7: to create a cost-effective data pre-processing service that refines, integrates and stores real-time data streams from instruments and sensors within primary storage into DART secondary storage so that data stored in secondary storage will be available to higher layers of the DART architecture for analysis and processing;
- SI8: to establish a pilot data transfer service between secondary storage repositories (particularly between James Cook University and Monash University) which can deal with the transfer of large volumes of data over long distances at high speed; and
- SI9: to determine the configuration and specifications required for a large storage infrastructure.

3.2.2 Content and Rights (CR)

The CR work packages examine methods, technologies and incentives to address the concerns researchers have in relation to submitting their research and data into institutional repositories. Ultimately, this work package group aims to increase data deposit rates into DART storage systems.

Creative Commons: The Creative Commons project allows owners of data to attach standardised licences to their data.⁹

Science Commons: a new Creative Commons project that is investigating the legal and technical mechanisms required to enhance scientific information sharing and will develop software that allows scientific researches to attach standardised licences.¹⁰

The specific objectives of these work packages are as follows:

- CR1: to examine issues that act as a barrier to moving data from personal data repositories to secure trusted alternatives (including trust, security and intellectual property issues);
- CR2: to promote content acquisition by providing non-science researchers with more rights-assignment options in relation to their research data (including investigating the application of the Creative Commons work to non-science research data and results, and then integrating this into software);

- CR3: to promote content acquisition by using the Science Commons to provide science researchers with additional rights options;
- CR4: to enhance information management practice by placing information management professionals into particular research communities;
- CR5: to provide software that makes it easy for researchers to deposit digital objects into repositories; and
- CR6: to increase deposit rates by identifying and examining the relevant legal issues (other than those considered in packages CR2 and CR3) that arise from the deposit of information into institutional repositories, as well as its subsequent storage, dissemination and use.

3.2.3 Annotation and Assessment (AA)

This group focuses on establishing tools and services that will allow users to attach opinions, reviews, comments or assessments to research data, publications, reports and other digital objects stored in DART repositories.

Wiki: a 'type of Website' that allows users to easily add and edit content and is especially suited for collaborative writing.¹¹

Plone: a web content management system that can be used for project groups, web sites, communities, intranets and extranets.¹²

Weblog: an online journal or diary.¹³

Vannotea: a collaborative annotation tool which allows text, images, web pages and threaded discussions (for example, entries of questions and answers) to be attached to digital objects.¹⁴

Those within collaborations will also be able to make real-time annotations and contributions to digital objects such as videos, images and 3-D objects, as well as Wikis. The DART project will integrate Wiki technology into the SRB, which will enable the Wiki to provide commentary on, and be the interface to, data grid management systems, distributed file systems, digital libraries and semantic webs. Ultimately, the various DART annotation and assessment tools will provide an alternative or additional means for the peer-review of research outputs.

The DART project has its own Plone Wiki/Weblog. DART general information and document searches can be conducted on the site. Individuals working on the project can also place daily blog entries on the Plone Wiki/Weblog that

are accessible to others working on the project. This enhances communication between work groups and enables the community to access general information about the project.¹⁵

To enhance the review process, DART will provide users with the use of Vannotea. This tool allows users to search for certain annotations. Collaborators can communicate through an online conference room, where each user's actions in relation to digital objects can be recorded and seen simultaneously by other participants. Vannotea also includes a web browser that can be used to access existing audio-visual archives.

The AA work packages have the following objectives:

- AA1: to develop annotation tools and services that will allow researchers to annotate their peers' work;
- AA2: to allow end-user control over who can make annotations to their work and who can access these annotations;
- AA3: to provide tools that will allow groups to make collaborative annotations to digital objects during application sharing in access grid sessions or videoconferencing. This work package will also develop tools that will allow asynchronous annotations by groups; and
- AA4: to integrate SRB with Wiki technologies and pilot this new mechanism for Wiki-based collaborative practice in research teams.

3.2.4 Discovery and Access (DA)

The aim of the DA group of work packages is to develop tools and services that will allow users to browse, search, discover and access resources within repositories. Access to items stored in DART repositories will be either unrestricted or controlled in some manner, depending upon the specific needs of the persons and organisations who deposited these items.

The tools and services that are being developed under the DA work packages include portals that will provide interfaces across distributed archives, ontologies and a semantically-augmented MCAT RDF data store that will allow semantic interoperability between heterogeneous metadata schemas. A centralised repository or registry of ontologies and metadata schemas is also being created.

JISC IE Metadata Schema Registry Project (IEMSR): a project funded by the Joint Information Systems Committee (JISC) is developing a metadata schema registry as a pilot shared service within the [JISC Information Environment](#).¹⁶

The intended outcomes of the DA work packages are as follows:

- DA1: to develop software that will allow end-users to control who can access their work;
- DA2: to enhance the discoverability of information by integrating DART repositories and other repositories with the National Library of Australia's national research discovery service;
- DA3: to create a centralised repository or registry of metadata schemas which will build on work carried out on the IEMSR project.

3.3 DART DEMONSTRATOR MODELS

Three demonstrator model projects have been chosen to highlight how the tools established under the DART project work packages can be used in practice. The aim is to provide a 'proof of concept' for certain tools created under each work package. The Crystallography and Climate Research demonstrator models illustrate how researchers in the science disciplines can utilise DART tools, while the Digital History Demonstrator will illustrate how the humanities disciplines can also benefit from the project. Each model is discussed in turn below.

3.3.1 X-Ray Crystallography Demonstrator Model

What is X-ray crystallography?

X-ray crystallography is a technique that uses X-ray beams to obtain a 3D model of the subatomic structure of a molecule. Crystallography, which concerns the study of crystals,¹⁷ has been described as 'the science of the structure of materials'.¹⁸ The X-ray crystallography process involves creating a crystal of the relevant substance under investigation. A crystal is 'a regular, repeating array of atoms or molecules in three dimensions'.¹⁹ X-ray crystallography uses crystals of the molecule to be studied because the molecule in isolation is too small.²⁰ The crystal is then bombarded with X-ray beams, which are diffracted by the atoms in the crystal. The X-ray diffraction pattern is recorded and is used to determine the relevant structure.²¹

X-ray crystallography experiments can be conducted at laboratories with the necessary equipment, or at synchrotron facilities. Synchrotron radiation provides more intense X-rays than are available in X-ray diffraction laboratory facilities. Australian crystallographers currently visit overseas synchrotron facilities, such as those at the Advanced Photon Source in Chicago. However, an Australian synchrotron is currently being built at Monash's Clayton campus and is scheduled for completion in 2007.

What is the aim of the model?

All three DART partner institutions have X-ray crystallography laboratories that are engaged in the DART x-ray crystallography demonstrator model ('crystallography demonstrator'). The crystallography demonstrator initially aims to enhance and improve the access of the DART partners to the three respective crystallography laboratory facilities. The wider goal is to develop more advanced data collection, storage, analysis and publication tools to overcome limitations in the current X-ray crystallography research process.

The current X-ray crystallography research process

The following steps are involved in the X-ray crystallography process:²²

1. A small crystal of the relevant structure is prepared (less than 1mm). The crystal is usually made by placing the molecule in solution and allowing it to crystallise through vapour diffusion over a period of time;
2. The crystal is placed in an X-ray beam and a 3-D diffraction pattern is obtained via the collection of a series of images captured by a charge-coupled device (CDD device)²³ as the crystal is rotated;²⁴
 - While the CDD device is the primary sensor, other environmental variables are collected, including the crystal temperature, X-ray source cooling status, experiment times, ambient temperature and humidity;
 - The experiment also relies on an actuator:²⁵ the crystal is moved precisely through the X-ray beam by the goniometer, which is a three degree of freedom positioning system;
3. The diffraction pattern is then used to determine the structure of the protein via a process of computer processing and modelling.²⁶ Either the X-ray crystallography facility, or the researcher that requested the experiment can perform this analysis.
4. Researchers will frequently deposit the complete structure in a public crystallographic database such as the RCSB Protein Databank (PDB) which stores the three-dimensional structures of large biological molecules²⁷

Limitations of the current X-ray crystallography research process

No remote access to instruments. X-ray diffraction instruments are expensive and require a highly trained operator. These instruments are usually only available at universities or colleges and national synchrotron facilities. It is not possible with current technology for a scientist working off-site to access or interact with the instruments.²⁸ Researchers who wish to observe the experiments usually prepare the crystal samples and travel with them to the desired X-ray crystallography or synchrotron facility.

Inadequate facilities for storage of data. The development of instrumentation in the area of single crystal X-ray diffraction has significantly increased the quality and quantity of data, particularly in the area of X-ray detector technology.²⁹ However, the data collection and archival procedures are not developing at the same rate. Currently, data must be transferred from the instrument data acquisition machine to other post-processing facilities and is then archived on other media such as a DVD or CD.

The DART X-ray crystallography research model

The DART crystallography model aims to improve the current research process in the following way (see also Figure 3.3 below):³⁰

1. Collect Data

- Remote users, as well as users located at a participating X-ray crystallography facility, can submit their crystal to be analysed at the relevant facility (see the discussion of possible users of the demonstrator below). If a remote user is involved, the user must send a crystal sample to the remote crystallography facility;
- The user is notified when the facility will run the experiments on the sample;
- An individual in the laboratory (which may also be the user) adjusts the scanning parameters for each X-ray diffractometer scan by physically adjusting the crystal and a camera within the X-ray diffractometer;
- The experiment proceeds as described above. However, as well as the collection of experimental data values and CCD images, the DART procedures will include live feeds of video footage of the relevant laboratory and the mounted crystal, while still images will be taken from this footage that can be viewed in succession. These forms of data will be available to authorised users as outlined below;
- The relevant user will be able to monitor the status of the experiment by selecting the appropriate instrument/s via

GridSphere, which is a Web portal.³¹ As well as viewing the video footage and still images, the user will be able to view real-time statistical data and real-time diffraction data. Statistical data will include (but will not be limited to) Scan Time, Scan Resolution and Scan Angle. Real-time diffraction data will include (but will not be limited to) Crystal Temperature, Ambient Temperature (Laboratory), Liquid Nitrogen Remaining, and crystal diffraction images;

- Only users who have a relevant username and password are permitted access to GridSphere;
- It is envisaged that relevant users will have remote access to many instruments and sensors, including diffractometers and synchrotron beamline settings (NOTE: the demonstrator will not implement direct remote control of instruments); and
- DART will provide distributed operation of the data acquisition system.

2. Manage Data

- Users can choose to store raw data from instruments in a local file system, a Storage Resource Broker (SRB)³² or an archival mass storage system. For example, the Monash University Whisstock X-ray crystallography laboratory will be using supercomputing space provided by the Monash Sun Grid to store their data.³³ GridSphere will be the interface for DART data storage. Each partner institution will have its own Data Manager and SRB storage facility that will be federated across the other institutions' sites; and
- Annotations and metadata are automatically added to the data set as the data is processed.

3. Analyse Data

- The relevant user will be able to access their raw data via GridSphere and transfer the data to a local machine;
- The relevant user can evaluate the data using the crystallography analysis software, Mosflm. If the data is acceptable, the user can locally analyse the data and collaborate with others using the CCP4 program suite;³⁴
- Analysed data can be uploaded into GridSphere;
- The relevant user can download analysed diffraction data from GridSphere onto a local machine to establish the structure of the crystal and to develop a three-dimensional model of the protein. The user can collaborate with other parties and use programs such as PyMOL to establish the relevant structure;

- The relevant user can upload the protein structure into GridSphere; and
- Relevant users will be able to add annotations to the data and three-dimensional representation during the analysis process.

4. Manage Information

- Relevant users will archive the results of the experiment and the relevant analytical procedures after analysis and structure determination; and
- Annotations that relevant users add to the raw and analysed data will be automatically added to the experimental record.

5. Collaborate and Annotate

- Relevant users will be able to work collaboratively with others in their research group to analyse and annotate raw and analysed data.

6. Publish Information

- The relevant user can download relevant files from GridSphere and collaborate with others in their research group to create a publication;
- Publications can purely illustrate the results of the X-ray crystallography, or can include comments and analysis;
- The publication and any relevant data sets can be uploaded into GridSphere;
- The user can submit the publication to an open repository such as the PDB;
- The user can submit the publication and data into a closed repository using VALET. VALET is a web-based interface that enables the submission of electronic theses and dissertations into a FEDORA digital object repository;³⁵
- Once the PDB, or other repository reviews, accepts and publishes the user's findings, the user can unlock their publication and data on VALET; and
- The user can archive the publication and relevant datasets through GridSphere, enter metadata and submit the relevant files into the VALET repository.

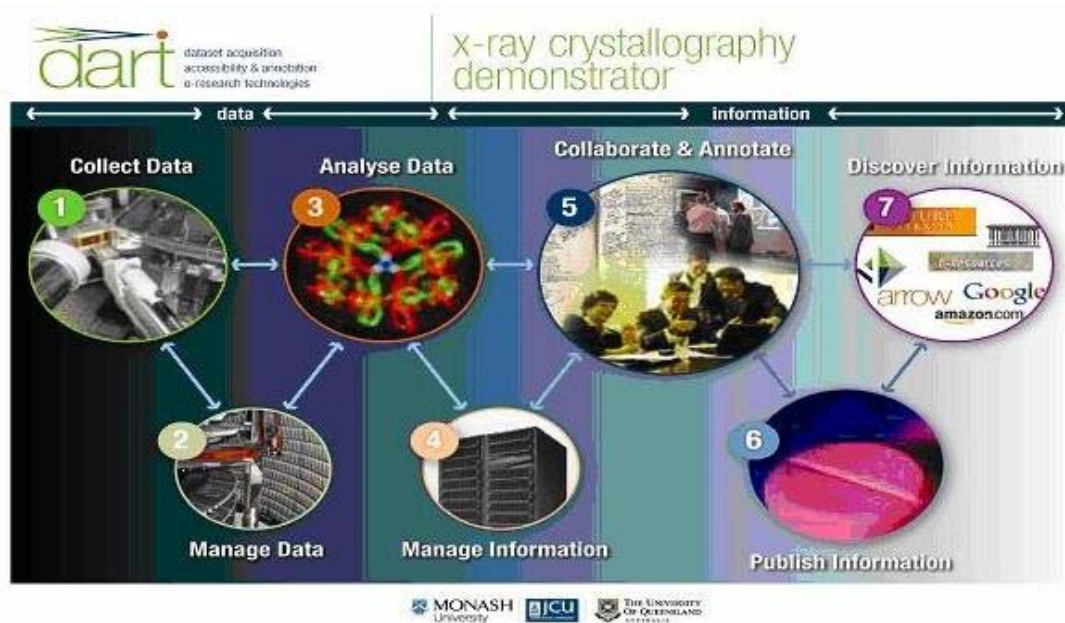
7. Discover Information

- Authorised users will have access to relevant data and publications through the GridSphere. Data will be available online from the collection to publication stages;
- Reviewers and possibly readers of the final publication may also have access to the relevant raw data; and
- DART will manage access rights, intellectual property issues and security.

Administration of GridSphere and JAINIS

Administration tasks can be undertaken through GridSphere for both GridSphere and the JCU And Indiana Instrument Services ('JAINIS'). The Systems Administrator (see description below) can log into GridSphere and use administration tools to administrate the portal, perform maintenance and other relevant activities. Similarly, the Technician (see description below) can log into GridSphere and use administration tools to perform any required activities for JAINIS. The precise administration tools that will be provided under the portal are yet to be determined.

Figure 3.3 - X-ray crystallography CCD image³⁶



Relevant Users of the Crystallography Demonstrator

The relevant users of the crystallography demonstrator will be:³⁷

- a **Senior Researcher** – this user will be any person who heads a research team or that has been given additional rights by the Experiment Administrator (see below). The Senior Researcher will have a high standard of usage rights, which will include the ability to access and monitor their own data, as well as the data of other members of their team. The Senior Researcher will also be able to access data management tools. This user will be able to perform all the tasks as described above from point 1 to 7 for their own and their team's data.
- b **Researcher** – this user will be any person that uses the equipment and tools in the crystallography laboratory (such as the Whisstock Laboratory at Monash University) to analyse crystals. The rights of the researcher are standard and include the ability to access and monitor their own data, as well access data management tools. This user will be able to perform all the tasks as described above from point 1 to 7 for their own data.
- c **Student Supervisor** – this user will be any person who supervisor's a Student Researcher's thesis (see below). The Student Supervisor generally has the same rights as a Researcher, although this user also has rights in relation to viewing a Student Researcher's data. Accordingly, this user will be able to perform all the tasks as described above from point 1 to 7 for their own data, as well as view their Student Researcher's data.
- d **Student Researcher** – this user will be an Honours, Masters or PhD student that is undertaking a thesis within the relevant laboratory. The rights of a Student Researcher are limited, as they are only permitted to monitor and access data relevant to their own experiments. Therefore, this user will be able to perform all the tasks as described above from point 1 to 7 for their own data.
- e **Experiment Administrator** – this user will be the Head of the relevant laboratory, or person that supervises the laboratories' activities. The rights of an Experiment Administrator are broad and include the ability to monitor and access data relating to any of the experiments that they supervise. The Experiment Administrator is also able to use data management tools and certain administration tools. This user will be able to perform all the tasks as described above from point 1 to 7 for all the data relating to the experiments they supervise.

- f **Corporate User** – this user will be any associated third party that has a commercial interest in the outcome of a certain experiment. The rights of a Corporate User will be limited, as they will only have access to particular pieces of data and real-time information and will have restricted access to GridSphere. Corporate Users will only be able to log into GridSphere, select the relevant instrument and view certain real time data.
- g **Systems Administrator** – this user will be the main GridSphere contact in the relevant laboratory. The Systems Administrator will only be able to access administration tools concerning the portal, maintain the portal interface and undertake other relevant tasks. This user will not have access to data unless they have been authorised by the Experiment Administrator and does not have access to the same administration tools as the Technician.
- h **Technician** – this user will be the main JAINIS contain in the relevant laboratory. The rights of the Technician will be to access administration tools for JAINIS, maintain JAINIS, access live experiment data, and undertake other necessary tasks. The Technician has access to different administration tools than the Systems Administrator.

3.3.2 Climate Research Demonstrator Model

The DART project is also working with climate research groups to demonstrate how the project can assist researchers in this area. Climate research concerns the study of the climate, which is defined as the average weather conditions over at least a thirty year period.³⁸ All three partner universities are involved in establishing this demonstrator model. However, each institution is integrating DART tools into their own distinct climate research projects.

The climate demonstrator has not been developed as fully as the crystallography demonstrator and there are still many uncertainties as to what specific research will be involved in the actual climate demonstrator. The description below omits any detail about the work at University of Queensland or how each climate group will use DART access and annotation tools. These will be included in our Final Report.

Monash University climate research demonstrator

It is expected that the Climate Research Group at Monash University will be using the tools provided by the DART project to assist in their analysis of climate data.

The Group's current research includes the creation of climate models in the form of grid maps that indicate climate values over a period of time. For example, research may be conducted in relation to rainfall in a particular area over 50 years, or the correlation between coral bleaching and climate data. The raw data on which these models are based includes the following:

- Sea Surface Temperature ('SST') data provided by the Australian Institute of Marine Science ('AIMS') in partnership with James Cook University. This data is obtained from a weather tower at Davies Reef in Queensland;
- Climate data from international sources; and
- Other data from international sources such as position coordinates, coral bleaching and temperature.

The Group currently stores their data in the Monash Sun Grid, which can be used for the analysis of the raw data requiring a high level of computational power. In relation to the DART project, the Group may utilise DART analysis and simulation tools through a portal that may be established under the project. At this stage, it is not known what precise tools that the Group will utilise, or whether the Group will make use of DART databases.

James Cook University (in collaboration with AIMS) climate research demonstrator (Davies Reef Environmental Sensor Network)

This work involves collaboration between JCU and AIMS in relation to the tower situated at Davies Reef. JCU has established a sensor network over the reefs that surround the weather tower. These sensors collect readings concerning sea temperature, air temperature and air pressure. A web camera will be placed on the weather station to collect images of the area. JCU will also be remotely monitoring sensors placed on the weather tower to assess the status of the batteries for the system. The data obtained will be transmitted to the mainland over a high speed microwave link.³⁹

The data collected from the sensors and the web camera will initially be stored in AIMS storage facilities. It is intended that the data will be

transferred as needed for applications that require it. It is expected that the data will initially be used mainly by Australian tertiary institutions but at this stage this aspect is unlikely to be a major component of the demonstrator model.

3.3.3 Digital History Demonstrator Model

The third demonstrator model, the Digital History demonstrator, has been chosen for the DART project to illustrate and investigate the use of DART tools in the humanities. Each of the three partner institutions has selected their own humanities project as part of this demonstrator.

Women on Farms Heritage Collection Project – Monash University

The Women on Farms Project is a partnership between Monash University (Faculties of Information Technology and Arts), Museum Victoria and the Women on Farms Gathering community. The Project collects and collates information from Women on Farms Gatherings, which have been held annually in Victoria since 1990. The project intends to establish a portal that contains the Women on Farm Gathering Collection.⁴⁰

The information from the Gatherings is collected with the help of curators from Museum Victoria. The women participating in the Gatherings write up their stories and send them to the museum. The museum also conducts interviews and records the meetings. The recorded information and interviews are stored in digital form, and can be text, images, audio files or videos. The collection of information is also overseen by a Heritage Group, which is comprised of Gathering representatives. The Group identifies and assesses relevant materials to be included in the collection.⁴¹

The information contained in the portal is currently available only to members of the three partner organisations and other researchers from the community. It is envisaged that use of the data by the partner organisations will be governed by a collective research agreement. The main Monash University research groups involved with the project are the Faculty of Arts research group on History and Women Studies and the Faculty of Information Technology research group on Community Informatics and Collaborative Design Principles/Processes. One of the partner organisations, Museum Victoria, intends to export the data into its own database. The information will also be made available to the University of Otago in New Zealand, which is conducting geographical, farming and rural studies⁴²

Although access to the collection is currently restricted, the Women on Farms portal will be connected to the Internet, so that the collection will eventually be generally accessible. The DART project will expedite this by:

- providing storage for the data collected by the project;
- managing access to the portal;
- providing annotation and other collaboration tools; and
- providing publication tools.

Relevant users of the portal will be able to utilise the tools developed by the DART project via a GridSphere portal. At present, the relevant users of the portal are envisaged to be:⁴³

- Museum Researcher** – this user will be a curator working in the Museum, who has an interest in the creation and curation of the objects within the portal. The user will also be interested in using the stories provided by members of the community via the portal to enhance the Museum's collection.
- Community Researcher** – this user will be any researcher who is studying community informatics. The user may be a researcher from the information technology faculty, a researcher from another university, or a research representative of the community.
- Student Researcher** – this user will be undertaking postgraduate research as an Honours, Masters or PhD student and will be working in the Museum. The user predominantly contributes in relation to public history and will have limited rights over the collection.
- Arts Researcher** - this user may also be a supervisor of a student researcher. Therefore, this user will have access to their student's contributions.
- Systems Administrator** – this user will be the main administrator of the portal. The Systems Administrator will have access to all administration tools in regards to the portal. The user will maintain the portal interface and undertake other important tasks. This user will not have access to data unless they have been given authorisation.

The Nelson Report Project – University of Queensland

The aim of this project is essentially to digitise the N.F. Nelson Report. This report was written by Norman F. Nelson who, in 1936, was commissioned by the Presbyterian Church to visit and report upon four Presbyterian Church missions at Weipa (Napranum), Mapoon, Aurukun and Mornington Island in Cape York.

As a result, Nelson produced this valuable report, which is officially entitled 'Record of Visit to Mission Stations 1936'. The report contains over 1000 annotated photographs of the indigenous children, the missionaries and staff that lived and worked at the missions, and other locations, such as Burketown and Cloncurry. The report also includes photographs of the missions' grounds and buildings, as well as maps, plans and a typescript diary concerning daily life at the missions. The report was bound into one book.

The report is currently held in the Fryer Library at the University of Queensland. Copies of the photographs are also held at Queensland Presbyterian Historical Records, which is the Presbyterian Church of Queensland's archives unit.⁴⁴

Digitisation is required to preserve the report as the hard copy version of the photographs and the negatives produced for the report are beginning to deteriorate. In addition to preserving the report, digitisation will make the report more accessible to the subjects, their families and indigenous communities in Cape York.

Increasing the accessibility of the report, however, poses particular difficulties, as the report contains sensitive, private and sacred information that members of the indigenous community may wish to keep private. This means that strict conditions may need to be imposed on access to the digital material.

The DART project will assist in the process of digitising the report, and making it more accessible, by:

- implementing authentication mechanisms that will ensure conditional access to the digital photographs and other material;
- indexing the collection and creating user-friendly interfaces that will allow the relevant indigenous communities to easily browse, search, retrieve and print photographs and annotations; and
- provide oral and textual annotation tools to allow authorised users to attach names to people, events and locations in the photographs, and to attach their own descriptions and stories.

It is also intended that additional collections and information sources of historical and cultural importance to the Western Cape York communities will be integrated into the project.⁴⁵

Gugu Badhun Digital History Project - James Cook University

The aim of this project is to record and display the life histories of elders of the Gugu Badhun people and non-Indigenous people who consider the upper Burdekin region a place of long-standing emotional and cultural significance. The project is being conducted by researchers at James Cook University and Gugu Badhun Ltd.⁴⁶

At the time of writing this Interim Report, details of how the DART project will be involved in the Gugu Badhun Digital History project were unavailable.

ENDNOTES

¹ Figure 3.1 can also be found at: DART, *DART presentation to DEST, March 30 (updated)* (2006) <<http://plone.jcu.edu.au/dart/Members/JeffMcDonell/presentations/DART%20and%20ARCHER%20Presentations/DART%20March%2030%20talk/view>>.

² This figure builds upon work described in H Van de Sompel, S Payette, J Erickson, C Lagoze and S Warner, 'Rethinking Scholarly Communication: Building the System that Scholars Deserve' (2004) 10 No. 9 *D-Lib Magazine* <<http://www.dlib.org/dlib/september04/vandesompel/09vandesompel.html>>. Figure 3.2 is also found in: DART, *DART Bid Document (public version)* (2005) <http://www.dart.edu.au/DART_Bid_Document.pdf>.

³ Common Instrument Middleware Architecture: *instrument-middleware.org, CIMA* (2005) <<http://www.instrumentmiddleware.org/metadot/index.pl?iid=2119&isa=Category>>.

⁴ SRB, *FAQ* (2006) <<http://www.sdsc.edu/srb/index.php/FAQ>>.

⁵ DART, *DART Bid Document (public version)* (2005) <http://www.dart.edu.au/DART_Bid_Document.pdf>.

⁶ Fedora, *Fedora Digital Repository System* (2006) <<http://www.fedora.info/documents/brochure/Fedora%20Page%20Final.htm>>.

⁷ For example, SRB, GFarm and Globus. Information on GFarm can be found at: Grid Datafarm, *Gfarm file system* (2006) <<http://datafarm.apgrid.org/>>. Information on Globus can be found at: The Globus Alliance, *About the Globus Alliance* (2006) <<http://www.globus.org/alliance/about.php>>.

-
- ⁸ This implementation is based upon Nimrod/G and GriddLes software. Information on Nimrod/G can be found at: Nimrod, *Nimrod/G* (2005) <<http://www.csse.monash.edu.au/~davida/nimrod/nimrodg.htm>>. Information on GriddLes can be found at: Grid Enabling Legacy Software: GriddLes, *Home* (2005) <<http://www.csse.monash.edu.au/~davida/griddles/>>.
- ⁹ Creative Commons, *Learn More about Creative Commons* (2006) <<http://creativecommons.org/learnmore>>.
- ¹⁰ Science Commons, *Science Commons* (2006) <<http://sciencecommons.org/>>.
- ¹¹ Wikipedia, *Wiki*, (2006) <<http://en.wikipedia.org/wiki/Wiki>>.
- ¹² Plone™, *What is plone?* (2006) <<http://plone.org/about/plone/>>.
- ¹³ A 'Weblog' can also be referred to as a 'blog': bytown internet, *Glossary* (2006) <www.bytowninternet.com/glossary>.
- ¹⁴ The University of Queensland Australia, *Vannotea* (2006) <<http://www.itee.uq.edu.au/~ereseach/projects/vannotea/index.html>>.
- ¹⁵ The Plone Wiki/Weblog is located at: DART, *Welcome to DART* (2006) <<http://plone.jcu.edu.au/dart>>. Access to the Plone Wiki/Weblog varies according to the user's certification.
- ¹⁶ JISC IE Metadata Schema Registry, *Home* (2006) <<http://www.ukoln.ac.uk/projects/iemsr/>>.
- ¹⁷ Giacovazzo et al, *Fundamentals of Crystallography* (1992) Preface.
- ¹⁸ Mark Ladd and Rex Palmer, *Structure Determination by X-ray Crystallography* (4th edition, 2003) xi.
- ¹⁹ A. Ducruix and R. Geigé (eds), *Crystallization of Nucleic Acids and Proteins, A Practical Approach* (2nd ed, 1999) 392.
- ²⁰ Protein Crystallography Unit (PCU), established in the School of Biomedical Sciences: Monash University, *Crystal crazy* (2006) <<http://www.monash.edu.au/pubs/monash-news/2004/crystal.html>>.
- ²¹ Giacovazzo et al, *Fundamentals of Crystallography* (1992) Preface.
- ²² Jeff McDonnell, 'DART Project Business Case' (Monash University, 2006) 3-4.
- ²³ A charge-coupled device is an image sensor that can be used to transfer electrical charge, create images of objects, or store information: Courtney Peterson, *How It Works: The Charged-Coupled Device, or CCD* (2001) <<http://www.jyi.org/volumes/volume3/issue1/features/peterson.html>>.
- ²⁴ See presentation: Monash University, *DART, developing toolkits for e-Research* (2006), available at: <<http://www.monash.edu.au/ereseach/resources/its-presentation-jm.pdf>>.
- ²⁵ An 'actuator' is a 'mechanism that causes a device to be turned on or off, adjusted or moved', see: PCMag.com, *Definition of: actuator* (2006) <http://www.pcmag.com/encyclopedia_term/0,2542,t=actuator&i=37479,00.asp>.
- ²⁶ See presentation: Monash University, *DART, developing toolkits for e-Research* (2006), available at: <<http://www.monash.edu.au/ereseach/resources/its-presentation-jm.pdf>>.

-
- ²⁷ This is 'the single worldwide depository of information about the three-dimensional structures of large biological molecules, including proteins and nucleic acids': RCSB Protein Data Bank, *Welcome to the RCSB PDB* (2006)
<<http://www.rcsb.org/pdb/home/home.do>>.
- ²⁸ Tharaka Devadithya, Kenneth Chiu and Donald F. McMullen, *The Common Instrument Middleware Architecture: Overview of Goals and Implementation*, Indiana University Computer Science Technical Report No. TR616 (2005)
<<http://www.cs.indiana.edu/pub/techreports/TR616.pdf>> 1-2.
- ²⁹ Tharaka Devadithya, Kenneth Chiu and Donald F. McMullen, *The Common Instrument Middleware Architecture: Overview of Goals and Implementation*, Indiana University Computer Science Technical Report No. TR616 (2005)
<<http://www.cs.indiana.edu/pub/techreports/TR616.pdf>>.
- ³⁰ Jeff McDonnell, 'DART Project Business Case' (Monash University, 2006) 4-5; Nicholas McPhee, 'DART Crystallography Demonstrator Use-Cases' (Monash University, 2006).
- ³¹ For more information on the GridSphere project, see:
<http://www.gridisphere.org/gridsphere/gridsphere>.
- ³² SRB, *Mainpage* (2006) <http://www.sdsc.edu/srb/index.php/Main_Page>.
- ³³ The Monash Sun Grid is a 'high-performance compute facility' available to Monash University researchers: Monash University, *Monash Sun Grid* (2006)
<<http://www.monash.edu.au/eresearch/activities/msg.html>>.
- ³⁴ For more information on this program suite and the Collaborative Computational Project Number 4 in Protein Crystallography (CCP4 Project), see: CCLRC, *CCP4* (2006) <<http://www.ccp4.ac.uk/about.php>>.
- ³⁵ For more information on VALET for Electronic Thesis & Dissertations (ETDs) established by Visionary Technology for Library Systems, Inc ('VTLS'), see: Visionary Technology in Library Solutions, VALET for ETDs (2006)
<<http://www.vtls.com/Products>>.
- ³⁶ Figure 3.3 can be found in the presentation: Monash University, *DART, developing toolkits for e-Research* (2006), available at:
<<http://www.monash.edu.au/eresearch/resources/its-presentation-jm.pdf>>.
- ³⁷ Nicholas McPhee, 'DART Crystallography Demonstrator Use-Cases' (Monash University, 2006).
- ³⁸ Climate Prediction Center, *Climate Glossary* (2004)
<<http://www.cpc.noaa.gov/products/outreach/glossary.shtml#C>>.
- ³⁹ DART, *Davies Reef Sensor Network* (2006)
<<http://plone.jcu.edu.au/dart/Members/CameronH2/daviesreef>>. Access to this resource is restricted according to user certification.
- ⁴⁰ Liza Dale-Hallett and Rhonda Diffey, 'Motherboards and desert sands: stories of Australian rural women' (2006) 27 No. 1 *Frontiers - A Journal of Women Studies* 90-115
<http://find.galegroup.com.ezproxy.lib.monash.edu.au/itx/retrieve.do?contentSet=IAC- Documents&resultListType=RESULT_LIST&qrySerId=Locale%28en%2CUS%2C%29%3AFQE%3D%28JN%2CNone%2C42%29%22Frontiers+->

[+A+Journal+of+Women%27s+Studies%22%3AAnd%3ALQE%3D%28DA%2CNone%2C8%2920060101%24&sgHitCountType=None&inPS=true&sort=DateDescend&searchType=PublicationSearchForm&tabID=T002&prodId=EAIM&searchId=R1¤tPosition=7&userGroupName=monash&docId=A152016258&docType=IAC](#)>. Internet resource is restricted to Monash University certified users.

⁴¹ Liza Dale-Hallett and Rhonda Diffey, 'Motherboards and desert sands: stories of Australian rural women' (2006) 27 No. 1 *Frontiers - A Journal of Women Studies* 90-115

<http://find.galegroup.com.ezproxy.lib.monash.edu.au/itx/retrieve.do?contentSet=IAC-Documents&resultListType=RESULT_LIST&qrySerId=Locale%28en%2CUS%2C%29%3AFOE%3D%28JN%2CNone%2C42%29%22Frontiers+-+A+Journal+of+Women%27s+Studies%22%3AAnd%3ALQE%3D%28DA%2CNone%2C8%2920060101%24&sgHitCountType=None&inPS=true&sort=DateDescend&searchType=PublicationSearchForm&tabID=T002&prodId=EAIM&searchId=R1¤tPosition=7&userGroupName=monash&docId=A152016258&docType=IAC>. Internet resource is restricted to Monash University certified users.

⁴² Stefanie Kethers, Nicholas McPhee and Natalie Pang, 'DART Project Some Issues around User Requirements' (presentation delivered at the DART Portal Workshop, 2 August 2006).

⁴³ Natalie Pang, 'Digital History: Women on Farms Gathering Community Use-Cases (Monash University, 2006).

⁴⁴ The University of Queensland Library Catalogue, *Record of visit to mission stations 1936 [manuscript]* (2005) <<http://library.uq.edu.au/record=b1974701>>.

⁴⁵ Project Description: Preservation and Repatriation of the N. F. Nelson Report through Digitisation (DART project internal document).

⁴⁶ James Cook University, Faculty of Arts, Education and Social Sciences, *Successful Grant Applications (current)* (2005) <<http://www.faess.jcu.edu.au/grants.html>>; James Cook University, *Annual Report 2004* (2005) <<http://www.jcu.edu.au/div1/registry/annualreport/AnRep2004web.pdf>>.

4 INTELLECTUAL PROPERTY

All the creative products of those who are involved in academic research are capable of legal protection under one or more of the areas of intellectual property (IP) law. These areas are known as copyright, patents, designs, trade marks, circuit layouts, plant breeder's rights and the equitable doctrine of breach of confidence. Each of these categories is broad and quite complex and most contain within their scope a number of subcategories of rights and subject matter.

The principal areas of IP that are discussed below are copyright and the action for breach of confidence. The law of patents may also be relevant to e-Research that is conducted using an infrastructure such as DART (and ARCHER). Patents are a statutory monopoly that are granted to new and inventive processes or products that are useful. If international protection is to be sought for an invention, it is necessary to keep the invention secret until a patent application is filed. Therefore, if research using the DART (or ARCHER) infrastructure may result in a patentable invention, it will be necessary for certain precautions to be taken to ensure the information remains secret.

This chapter will only provide a broad discussion of the aspects of the law relating to copyright and breach of confidence that are likely to be of most relevance to the DART project. It will also outline the types of creative products that may be generated at each stage of the DART project and identify the principal legal issues that might arise. The chapter will not discuss the aspects of the law relating to patents for inventions, although these will be developed in the final report if the response to the interim report seeks this further detail.

4.1 COPYRIGHT

4.1.1 Introduction

In a general sense, the term 'copyright' is used to refer to rights in creative ideas that have been expressed in writing, or some other material form. Copyright provides no protection for the ideas themselves. As with all forms of intellectual property, these rights are in something intangible which is in contradistinction to the property rights that exist in the physical things in which the ideas are embodied. For example, a person may have copyright protection in a novel that she writes but these are different rights from those that she or others may have in a tangible copy of the published book.

A wide variety of research material that is collected, stored, annotated and published using an e-Research infrastructure, such as that which is being created under the DART and future ARCHER projects, will have copyright

protection immediately upon its creation. No registration is necessary to gain the protection of copyright law in Australia.

It is important to identify the subject matter in which copyright subsists, the nature of the rights and who is entitled to exercise those rights in that subject matter. It is also important to recognise that the law provides certain rights to the public to use copyright subject matter without infringement. The complex nature of collaborative research means that these questions are not always simple to resolve.

This section provides a brief overview of the main principles of copyright law that are likely to be relevant in e-Research. Secondly, it describes some types of copyright subject matter that may arise using DART with reference to the demonstrator models. Thirdly, it raises some issues that can be identified only in general terms at this early stage of the proof of concept project known as DART.

Why is copyright important?

Copyright is important because:

- It is a statutory regime that provides a set of property rights in creative works that meet the criteria for protection
- The owner of copyright can prevent the unauthorised use of their rights
- The statutory framework contains a balancing of rights comprised in copyright so that some free public use is possible

Contract can be used to adjust the statutory balance of rights in different ways to suit the particular circumstances. There may be less incentive to place their research materials in electronic repositories if owner's rights are not adequately protected.

4.1.2 Legal protection

There is a strong international framework for copyright protection but the substantive norms for protection in Australia are provided by the *Copyright Act 1968* (Cth) (Copyright Act), the principal ones being:

1. The subject matter that can be protected under copyright;
2. The criteria for subsistence of copyright;
3. Authorship of works and the maker of other subject matter;
4. Ownership of works and other subject matter;

5. The exclusive rights of the copyright owner;
6. Duration of copyright protection; and
7. The rights of the general public to use copyright material without infringement.

The discussion below provides a brief overview of each of these principles of copyright law.¹

4.1.3 Subject Matter

The Copyright Act distinguishes between 'original works' which are created by individuals and require a human author and 'subject matter other than works' which often come into existence with the investment of producers such as record companies, television or film production companies and publishers and require no human author.

Works

Part III of the Copyright Act sets out the available protection for copyright in original works. The concept of a 'work' is defined in s 10 to mean a literary, dramatic, musical or artistic work. Excepting musical works, each of these is separately defined. Original works include such things as computer programs, tables, compilations and databases, paintings, drawings, engravings, photographs, musical and choreographic compositions. The basic criteria for protection are that there is a human author and that some level of originality is present.

Subject matter other than works

Sound recordings, cinematographic films, television broadcasts and sound broadcasts and published editions are protected under a different part of the Copyright Act (Part IV). These are known as subject matter other than works and do not require a human author or any minimum level of originality.

This type of subject matter will usually contain layers of copyright material. For example, a sound recording is protected in its own right. However, separate copyright is likely to subsist in the music (musical work) and lyrics (literary work) that are recorded. The significance of this is that permission to make a copy of the sound recording, for example, would also require the permission of the owners of any current copyright in the musical and literary works.

The Act also provides in Part XIA for limited protection to performers in their live performances.

←TIP

Researchers are both users and creators of copyright subject matter. They must therefore be careful not to infringe the rights of others in the process of creating new subject matter.

4.1.4 Criteria for protection

Each of the following criteria for protection is discussed in turn:

- Connection with Australia
- Recorded in a material form
- Originality (in the case of works)

Connecting factors

Protection arises when the work or other subject matter has been realised in some material or tangible form, such as a word document, book or sound recording, and so long as the claimant satisfies the relevant requirements of nationality or residence or first publication within Australia.²

Material form

Copyright is only available when the work or other subject matter has been reduced to some material form. Therefore, there is no copyright protection for an idea that is disclosed to another person in the course of conversation unless it has already been reduced to writing or some other material form such as a recording. A definition of 'material form' in s 10(1) makes it clear that electronic storage will satisfy this requirement.

←TIP

Copyright subsists immediately when the work is reduced to a material form. No formalities, such as registration, are necessary to gain protection

Originality

Literary, artistic, dramatic and musical works must be original to gain copyright protection under the Act. This merely means that:

- The work must originate with the author, and must not be copied; and
- It does not need to be novel or inventive.

There is no level of originality required for other subject matter such as sound recordings and films.

☛TIPS

It is possible to create an original work that is based upon existing copyright material. However, although the new work may itself have copyright protection, its creation may have infringed the copyright in any work on which it was based

For example, X has copyright in the description of an event. Y copies the description and incorporates it within her own more detailed description. Y would own copyright in her prose but has infringed X's copyright in the process of its creation.

4.1.5 Authorship of works and the maker of other subject matter

The 'author' and works

The author is the person who creates a work and every work must have a human author for copyright to subsist. More specifically, the author is regarded as the person who creates the elements of the work that have copyright protection (the expression) and who is responsible for first reducing that work into a material form. Therefore, if one person (X) provides an idea to another person (Y) who then develops the idea into a written article, only Y is the author for the purposes of copyright law. The term 'author' is undefined, except in relation to photographs, where it means the person who took the photograph.

Sometimes it may be impossible to find the author of copyright material. This may be because there is no human author – for example, this may be the case with certain computer-generated works. It may also be because the work is published anonymously or under a pseudonym. Creators may be unable to use these works - often referred to as 'orphan works' – when the author, and hence the owner, cannot be found.³

The Act provides various presumptions in regards to authorship of works in civil actions. Section 127(1) provides that the person whose name appears on a work shall be presumed to be the author of the work, unless it is established otherwise.⁴ Separate presumptions also apply to photographs (see ss 127(3) and (4)).

Joint authorship

A work is recognised as a 'work of joint authorship' where the authors combine their original expression into one work in a way that obscures their original contributions. This is to be distinguished from a work of co-authorship where the contributions remain separate from each other. An example of a co-authorship is a book of essays that are written by different authors. Authorship, and hence joint authorship, plays a pivotal role in vesting rights of ownership in copyright works.

Uncertain area of copyright law

The courts to date have compared works created with the use of computers to more traditional types of tools used by authors to create works.⁵ However, the more sophisticated the technology becomes, the more difficult it may be to analyse authorship or find an identifiable author. Issues of this nature will arise in the context of some of the demonstrator models for the DART project where data is collected automatically by programmed instruments. For example, a 1995 report of the Copyright Law Review Committee (CLRC) provided examples of what is referred to as 'computer-generated' works, namely works for which there is no author:

'satellite images of things such as weather patterns, vegetation, and geological formations. In many cases the data that makes up these images is collected automatically by remote sensors on satellites. The information is automatically processed by specialised computer programs and the final image down loaded or printed out in hard copy form either automatically or at the press of a button.'⁶

Copyright law in the United Kingdom defines a computer-generated work and provides that its author is the person who undertakes the arrangements necessary for the creation of the work.⁷ There is no definition of a computer generated work in the Act.⁸ Therefore, unless it is possible to satisfy the criteria for subsistence in particular circumstances, including the requirement for a human author, works of this nature will not have copyright protection.⁹

People can use that data freely to create their own original copyright subject matter unless contract or some technological protection method restricts their access to that data.

The 'maker' and subject matter other than works

No human author is required for copyright to subsist in subject matter other than works. Instead, sound recordings, films and broadcasts merely require someone to make that subject matter whereas a published edition must be published. In all cases, the maker or publisher can be either a human or a body corporate.

4.1.6 Ownership of works and other subject matter

It is the owner of copyright who can exercise the exclusive rights under the Copyright Act. The owner can retain those rights for exclusive use or can grant some or all of those rights to third parties such as other academics or publishers. The scope of these rights and the way in which they may be granted to others are discussed below.

The first owner of the work is:

- The author of the work [s 35(2)];
- The maker of the subject matter (Part IV Division 5).

Special provisions modify the general rule that ownership vests initially in the author of the work. These are set out in Table 4.1 below and include works created by employees of proprietors of newspapers and magazines, certain limited agreements to photograph, paint or draw and employee works in general. In particular, s 35(6) provides that an employer owns copyright in any work that the author creates in pursuance of the terms of her employment.

The importance of ownership

It is the owner of copyright who has the exclusive right to exploit copyright and to approve and control its use by others. Any unauthorised use may expose a person to an infringement action.

An agreement can modify any of these rules either before or after the creation of the work [s 35(3); s 197]. It is common for Australian universities to modify s 35(6) by agreement through terms contained in intellectual property statutes and policies that form part of the employment contract. Although it is usual for these to vest ownership of scholarly works such as articles and books in the academic author,¹⁰ there is no unified approach and it is important to establish where the various rights in copyright vest in each case. Some policies may vest ownership in either the author or the employer but retain certain rights for the other party by way of a non-exclusive licence.

It is possible to have co-owners of copyright, such as where there is a work of joint authorship. (s 10(1)) Another way in which people may become co-owners of copyright is where an author assigns an interest in the copyright to another person.

Table 4.1 Exceptions to the general rule of copyright ownership

Exception	Application	Section or Part under the Act
Employment exception	An employer will generally own copyright material created by an employee under terms of employment under a contract of service or apprenticeship	s 35(6) (works) Part IV, Division 5 (subject matter other than works)
Commission exception	Where subject matter is made at the request of a person for payment (commissioned), the commissioner may own copyright. This exception is limited in regards to works to the taking of photographs for a private or domestic purpose, the painting or drawing of a portrait or the making of an engraving	s 35(5) (photograph, painting or drawing of a painting, or an engraving) ss 97(3) (sound recordings) s 98(3) (films)
Crown exception	The Commonwealth or State is the copyright owner of material made or first published in Australia 'by, or under the direction or control of the Commonwealth or State'	ss 176, 177 (works) s 178 (sound recordings and films)
International Organisations	An international organisation is the owner of subject matter if it is made or first published by, or under the control or direction of the organisation	s 187 (works) s 188 (subject matter other than works)

	Regulation 26 of the <i>Copyright Regulations 1969</i> (Cth) refers to Schedule 12 for a list of International Organisations to which the Act applies	
Newspaper, magazine or similar periodical exception	<p>The proprietor of a newspaper, magazine or similar periodical is the owner of literary, dramatic or artistic works created by an employee where it will be included in the periodical.</p> <p>However, an employee retains ownership in regards to reproduction of the work:</p> <p>for inclusion in a book; or</p> <p>in the form of a hard copy facsimile made from a paper edition or other hard copy facsimile edition (press clipping services)</p>	s 35(4) (literary , dramatic or artistic works)

←TIP

Parties must resolve who should own any copyright material and how rights may be exercised by others before the material is created. If the author is not to be the owner of copyright, the parties must also resolve the extent to which an author is to retain moral rights. Contracts can then be drafted accordingly.

4.1.7 The exclusive rights of copyright

Copyright is a form of personal property and provides the owner with a bundle of exclusive economic rights that vary according to the nature of the subject matter. Any unauthorised use may expose a person to an infringement action. The exclusive rights are summarised in Table 46.2.

In the case of literary, dramatic and musical works, the exclusive rights include the rights to:

- Reproduce the work in a material form;
- Publish the work;
- Perform the work in public;
- Communicate the work to the public; and
- Make an adaptation of the work

The term 'adaptation' does not refer to any modification of a work but has specific meanings. For example, a dramatic version of a literary work in a non-dramatic form is an adaptation of that literary work and vice versa. Also, an adaptation of a musical work is an arrangement or transcription of that work. (s 10(1))

In simple terms, the concept of communication to the public refers to making the work available online or through its electronic transmission as may occur when a person emails a document to another person. The inherent nature of artistic works results in fewer rights – there is no right to perform the work in public or to make an adaptation of the work.

The exclusive rights in other subject matter protect principally against unauthorised copying but extend, in the case of sound recordings and films, to include communicating the subject matter electronically, such as making the recording or film available to the public online.

The copyright owner can exercise any or all of the various exclusive rights himself, can license or permit others to do so [s 13(2)] or can assign any or all of the rights to others [s 196].

	<p>to communicate the recording to the public;</p> <p>to enter into a commercial rental arrangement in respect of the recording; and</p> <p>to authorise the doing of any of these acts.</p>	s 13(2)
Cinematographic films	<p>to make a copy of the film;</p> <p>to cause the film to be seen and/or heard in public;</p> <p>to communicate the film to the public; and</p> <p>to authorise the doing of any of these acts.</p>	<p>s 86</p> <p>s 13(2)</p>
Television and sound broadcasts	<p>to make a film or sound recording of the broadcast or a copy of that film or sound recording;</p> <p>to re-broadcast or communicate the broadcast to the public otherwise by broadcasting it and;</p> <p>to authorise the doing of one of these acts.</p>	<p>s 87</p> <p>S 13(2)</p>
Published edition of a work or works	<p>to make a facsimile copy of the edition; and</p> <p>to authorise the doing of this act.</p>	<p>s 88</p> <p>s 13(2)</p>

The usual way in which a person is authorised to exercise any of the exclusive rights of a copyright owner is through contractual arrangements that involve the grant of a non-exclusive, sole, or an exclusive licence. A non-exclusive licence means that the copyright owner can continue to exercise rights himself and can grant as many additional licences as he deems appropriate. A sole licence is one where the copyright owner shares the exclusive rights with the sole licensee. The copyright owner agrees not to grant another licence to anyone else.

An exclusive licence is defined as a licence that authorises the licensee (the person obtaining the licence) to exercise an exclusive right 'to the exclusion of all other persons' including the copyright owner (s 10(1)). Exclusive

licences must be in writing and signed by or on behalf of the owner, or prospective owner (s 10(1)).

Assignment

Exclusive rights can also be assigned under the Act (s 196). An assignment of the entire bundle of rights that comprise copyright from one person to another makes the assignee the new copyright owner. Assignments must also be in writing and signed by or on behalf of the person assigning copyright (s 196).

The bundle of rights in copyright can be divided up in any number of ways. For example, assignments can be made to apply to one or more classes of acts, apply for a set amount of time, or apply to a certain geographical area in Australia. An assignment can also be made for copyright subject matter that has not been created yet (this is referred to as 'future copyright') (s 197).

4.1.8 Moral rights

The Copyright Act confers certain non-economic rights known as moral rights on the individuals who are the authors of works and cinematograph films. (Part IX). These rights exist independently of the economic rights comprised in copyright. In contrast to the economic rights, moral rights are not transmissible to others. [s 195AN(3)] Therefore, it is possible for the economic rights to be owned by one person while the moral rights remain with the author.

There are three moral rights, namely:

- The right of attribution of authorship (Division 2);
- The right not to have authorship of a work falsely attributed (Division 3); and
- The right of integrity of authorship of a work (Division 4).

A 'work' for the purposes of this Part of the Act means a literary, dramatic, musical or artistic work or a cinematograph film. Authors can waive their rights in a written consent. [ss 195AW – 195AWB] With the exception of the right of integrity of authorship in a cinematograph film (which continues in force until the author dies), moral rights continue in force until copyright ceases to subsist in the work. (s 195AM). At the date of this interim report, performers have no moral rights.¹¹

Complex provisions in the Act detail the circumstances in which someone might infringe moral rights and the circumstances in which a defence to infringement may apply. (Part IX, Division 6)

Why might moral rights be relevant?

As moral rights are separate from the economic rights in copyright, they may have different owners.

← TIP

It is important to obtain clearances for both economic and moral rights if copyright works are likely to be used in ways that would otherwise infringe moral rights.

4.1.9 Performers' Rights

Part XIA of the Act provides performers with rights in their live performances of musical, dramatic and literary works, dance, circus and variety acts and expressions of folklore. The rights in the performance are limited and do not extend to certain performances in educational institutions, performance of a sporting activity or participation in a performance as a member of an audience for example. The rights to prevent others from making or communicating unauthorised recordings.

Performers will also be co-owners of copyright in any sound recording of their live performance with the person who owned the record on which the recording was made. (ss 97, ss 22(3A), (3B)). However, in that case, and in the absence of the employer of the performer will own the performer's interest if the performance is made in pursuance of the terms of employment. (s 22(3B))

A performer can bring an action (s 248J) to restrain a variety of unauthorised uses of the performance that are specified in s 248G. These include among other things: recording a performance as a sound recording or film; broadcasting the performance; disseminating copies to the public over the internet; or making and selling copies of the recording of the performance.

Protection for a performance commences when the performance is given and generally continues for a period of 20 years from the end of that year. (s 248CA(1)).

4.1.10 Duration of copyright protection

The duration of copyright protection is dependent upon the nature of the subject matter, whether it is published and whether it is the subject of Crown copyright. *The US Free Trade Agreement Implementation Act 2004* extended copyright duration from 1 January 2005 for works, sound recordings and cinematograph films (other than those protected by Crown Copyright). For example, copyright in works now continues for 70 years (formerly 50 years) after the end of the year in which the author died. Table 4.3 outlines the duration of copyright protection which applies from 1 January 2005.

•TIP

If the author of a work has died, the duration of copyright protection depends upon when the work is published or made available to the public in some other way.

It is important to know the duration of copyright to determine whether it is possible to make free use of any subject matter. Particular caution is required where the subject contains more than one copyright protected work. For example, the copyright term for a sound recording of a song may have expired, but the copyright in the lyrics (literary work) and the music (musical work) may remain current. Therefore, although unauthorised copying of the recording will not infringe the rights in the recording itself, it will infringe copyright in both the literary and musical works.

Table 4.3 - Duration of copyright – 1 January 2005 -

Subject matter¹²	Duration	Section
Literary, dramatic, musical or artistic works	From the time made until end of 70 years after the end of the year of the author's death	s 33(2)
Literary (excluding computer programs), dramatic or musical works that have not been published, performed in public, broadcast, and records of the work had not been offered or exposed for sale to the public <u>before the death of the author</u>	From the time made until end of 70 years after the end of the year in which the work is published, performed, broadcast, or offered or exposed for sale (whichever event occurs first)	s 33(3)
Engravings unpublished at the time of the author's death	From time made until end of 70 years after the end of the year in which the engraving is first published	s 33(5)
Works that have been published anonymously or under a pseudonym	End of 70 years after the end of the year in which it was first published	s 34(1)
Sound recordings	From time made until end of 70 years after the end of the year in which the sound recording is first published	s 93
Cinematographic films made in Australia or by a qualified person	From time made until end of 70 years after the end of the year in which the film was first published	s 94(1)
Cinematographic films not made in Australia, not made by a qualified person, but first published in Australia	For 70 years after the end of the year in which the film was first published	s 94(2)
Television and sound broadcasts	Until expiration of 50 years after the expiration of the year in which the television or sound broadcast was first made	s 95
Published editions of works	Until expiration of 25 years after the expiration of the year in which the edition was first published	s 96

Literary, dramatic and musical works subject to Crown copyright (i.e. owned by the Commonwealth or a State)	From time the work is made until expiration of 50 years after the expiration of the year in which the work is first published	s 180(1)
Artistic works (excluding engravings and photographs) subject to Crown copyright	Until expiration of 50 years after the expiration of the year in which the work is made	s 180(2)
Engravings and photographs subject to Crown copyright	From time made until expiration of 50 years after the expiration of the year in which the engraving or photographs is first published	s 180(3)
Sound recordings and films subject to Crown copyright	From time made until the expiration of 50 years after the expiration of the year in which the sound recording or film is first published	s 181

4.1.11 Infringement of Copyright

Copyright provides the owner with exclusive rights that others might infringe when they copy the subject matter without permission. It is not necessary for the copying to be intentional. There will be no infringement unless a person creates something through direct or indirect copying that is substantially similar to the copyright subject matter.

Direct infringement (ss 36, 101) of copyright in arises when:

- A person who is not the owner of copyright;
- Who has no permission or licence from the owner;
- Does any act, or authorises (ss 36(1)(A), 101(1A)) another to do any act that is within the exclusive rights of the copyright owner (ss 31, 85-88);
- With respect to the whole or a 'substantial part' (s 14) of the work or other subject matter. Substantiality is assessed with reference to the quality of the part copied rather than the quantity of that part.

Two of these criteria, namely the concepts of authorisation and 'substantial part' require some further explanation. 'Substantial part' refers more to the quality of the amount taken, rather than the quantity.¹³ For example, in *Hawkes and Son (London) Ltd v Paramount Film Service Ltd*¹⁴ a newsreel

made of the opening of a school included approximately twenty seconds of a four-minute musical work 'Colonel Bogey's March' that was played by a band on the day. This inclusion was found to be an infringement of the musical work as the excerpt was highly recognisable and an essential part of the work. The originality of the part taken is another relevant factor for works in establishing whether a 'substantial part' was original.¹⁵ For subject matter other than works, where originality is not relevant, it remains the case that it is the quality of the part that is taken that is most important.¹⁶

The extension of the rights of the copyright owner to authorisation of the exercise of those rights allows a copyright owner to take action against either the person actually infringing their copyright or the person who authorised the infringing act. A copyright owner may want to take action against the authoriser when there are numerous or hard to identify users, or when the authorising person has more money or a more accountable public profile, or when taking action against the infringer may be unpopular.

The following factors are relevant when determining whether a person (X) has authorised infringement by another person (Y) (ss 36(1A), 101(1A)):

- The extent (if any) of X's power to prevent Y's infringing act;
- The nature of the relationship between X and Y; and
- Whether X took reasonable steps to avoid Y's act, including whether X complied with any relevant industry codes of practice.

Indirect infringement (ss 37, 38, 39, 102, 103, 107) refers to dealings with unauthorised copies of the protected material, such as by importing them or selling them in Australia.

In determining whether there has been a copyright infringement, it is irrelevant that the infringer created a new and original work. For example, reproducing a substantial part of a spare parts catalogue was found to be an infringement, even though the relevant part was used in creating a new and original work.¹⁷

Fair dealing and other exceptions to copyright infringement

Not all acts that fall within the exclusive rights of the copyright owner will infringe copyright. The Act provides a range of statutory exceptions that allow some degree of free use of the material or provision for the grant of a statutory licence. Some of these provisions will undergo significant reform as a result of the *Copyright Amendment Act 2006* (Cth).

At the currency date of this Interim Report, fair dealing exceptions apply for the following purposes:

- Research or study (ss 40, 103C);
- Criticism or review (ss 41, 103A);
- Reporting the news (ss 42, 103B).

The **Table 4.4** below includes a range of other exceptions from infringement and statutory licences that apply at the date of this Interim Report.

Table 4.4 – Principal Statutory Exceptions

Exception	Application	Sections
Fair dealing for research or study	Works or adaptations and audio-visual items (which under section 100A mean sound recordings, cinematograph films, sound broadcasts or television broadcasts)	s 40 (works); s 103C (audio-visual items)
Fair dealing for criticism or review	Works or adaptations of works and audio-visual items	s 41 (works) s 103A (audio-visual items)
Fair dealing for reporting the news	Works or adaptations of works and audio-visual items.	s 42 (works) s 103B (audio-visual items)
Fair dealing for the purpose of giving professional advice by a legal practitioner, trade mark attorney or patent attorney	Works and subject matter other than works. Note that the provisions for subject matter other than works do not refer to the exception as a 'fair dealing'.	s 43(2) (for works); s 104(b) and (c) (for subject matter other than works)
For the purpose of judicial proceedings or of a report of a judicial proceeding	Works and subject matter other than works.	s 43(1) (works); s 104(a) (subject matter other than works)

Temporary reproductions made as part of the technical process of making or receiving a communication, or using a copy of a copyright work	Works and subject matter other than works.	s 43A (works) s 43B (works) s 111A (audio-visual items) s 111B (subject matter other than works)
Acts concerning literary, dramatic and musical works	The reading of extracts from published dramatic or literary works in public or for broadcasting Performances at premises where people sleep or reside Reproduction of materials for broadcasting or simulcasting Sound broadcasts created by holders of print disability licences.	ss 45 – 47A
Acts concerning computer programs	Reproductions made for: Normal use Back-up copies Making interoperable products To correct errors and Security testing.	ss 47AB – 47H
Reproductions and communications conducted by archives and libraries	For example, for preservation and administrative purposes.	ss 48A-53 (works) ss 110A, 110B (subject matter other than works)
Acts concerning artistic works	For example, painting, drawing, engraving or photographing a sculpture or work of artistic craftsmanship situated in a public place, or including the work in a film or TV	ss 65 – 73

	broadcast.	
Acts concerning sound recordings	Causing recordings to be heard in public or broadcast; causing sound recordings to be heard in guest houses or clubs; making a copy of a sound recording for broadcasting or simulcasting	ss 105 – 109 s 110C
Acts concerning films	For example, causing a newsreel to be heard or seen in public 50 after the year the events depicted occurred; or Making a copy for the purpose of simulcasting	ss 110, 110C
Acts concerning broadcasts	Private and domestic use	S 111

The Copyright Amendment Act 2006 (Cth) introduces a new fair dealing exemption from infringement for use of copyright material for purposes of parody and satire (ss41A, 103AA). It also introduces a range of other exceptions that allow schools, universities, libraries and other cultural institutions to use copyright material for non-commercial purposes. These will be included in tabulated form in the final report.

Reproductions and communications conducted by archives and libraries

The Act also contains detailed provisions that permit libraries and archives to copy certain material without infringement. These exceptions from infringement enable the provision of copies for users, other libraries and archives and for purposes of preservation. Apart from official archives such as the Australian Archives, other collections of documents and other material that are of historical significance or public interest may also have the benefit of these exceptions from infringement. They must be in the custody of a body that is conserving and preserving that material on a non-commercial basis. (ss 10(1) and 10(4)).

4.1.12 General comments about copyright and the e-Research process

The principal copyright issues that arise at all stages of the e-Research process are to identify:

- a The relevant item – is it an existing copyright protected item that is to deposited into a DART depository or is it something that is created by annotating or otherwise using items (either protected by copyright or not) that are already in a DART depository?
- b Whether each item is a copyright ‘work’ or ‘subject matter other than works’ within the meaning of the Act;
- c In the case of a work, that it is original and has a human author;
- d The person or persons who are the owners of copyright in the subject matter;
- e That the person using the subject matter does so with the authority of the copyright owner; and
- f In the absence of the copyright owner’s express or implied authorisation, that the use falls within a statutory exception to infringement.

The identification of who owns copyright in specific material and the confirmation that relevant persons can use copyright material without infringement are therefore two critical aspects of the effective operation of e-Research using the DART model.

Some general principles apply to ownership of copyright material and should be considered across all aspects of the e-Research process. The vesting of ownership will depend upon the circumstances in which the relevant work is created and the contractual terms that govern that creation. There are multiple possible scenarios which can be condensed into a number of general categories:

- A. Copyright material that is deposited into the DART repository:
 1. Published and unpublished copyright material that is authored by the researcher and owned by the author. Non-exclusive rights may be granted to the employer pursuant to the terms of employment contained in the institutional intellectual property policy.
 2. Published and unpublished copyright material that is authored by the researcher and owned by the institutional employer. Non-exclusive rights may be granted to the author pursuant to the

terms of employment contained in the institutional intellectual property policy.

3. Published and unpublished copyright material that is authored by a number of people, only some of whom are employed. An example may be a computer program that is authored by an employed academic and her PhD student.
 4. Published and unpublished copyright material that is authored and owned by a third party who is outside any institutional collaborator. An example may be a photo from a private family album that is lent to a researcher.
- B. Copyright material that is created using the DART infrastructure and the contents of its repositories. Some examples include:
1. Laboratory experiments are recorded in a material form using DART infrastructure.
 2. Individuals annotate stored copyright items.

Having established where ownership will vest with reference to all existing statutory and contractual arrangements, it is necessary to identify how to allocate the rights in copyright through the use of contracts for the proper functioning of the demonstrator research models.¹⁸ Unless all likely copyright material and the circumstances of its creation are identified in a general sense in advance, the e-Research processes described in the DART project objectives may inadvertently infringe a copyright owner's exclusive rights. For example, if a researcher X deposits a copyright work that is owned by Y into a DART depository, X must not only have Y's permission to make this deposit but all possible uses of Y's work must also be identified in advance to ensure that the necessary licence is obtained. Any use that falls within a category of fair dealing or the scope of a statutory licence will not infringe, but there should be no general reliance in this new model of e-Research upon such exemptions from infringement.

Therefore, it is necessary to:

1. Check how any relevant agreements deal with ownership of copyright that is created or used in the course of the research. Employment contracts of authors that incorporate the terms of university intellectual property policies are of importance here.
2. Determine who may need rights in the relevant copyright material and the nature of those rights. For example, the collaborating institutions, the researchers, other users and those who assume legal responsibility for the operation of the DART infrastructure may require different

types of rights in order for the research to be conducted without inadvertent infringement of copyright.

3. Draft relevant contracts so that ownership will vest accordingly.. This may involve the need to seek a licence or assignment from the copyright owner before the material can be collected for storage, annotation and publication.
4. Draft licences to govern the extent to which any copyright work can be used by persons other than the copyright owner.

The consideration of copyright subject matter must include attention to the possible existence of moral rights and performers' rights, both of which are described in general terms above.

4.2 COPYRIGHT ISSUES ARISING AT SPECIFIC STAGES OF THE E-RESEARCH PROCESS

4.2.1 The Data Collection, Monitoring and Quality (DMQ) Assurance work packages (DART DMQ packages)

The DMQ work packages focus upon the generation and collection of 'raw' (unprocessed) research data using instruments and other devices such as sensors. The nature of the data is described below in the context of the crystallography and climate research demonstrator models.

Crystallography demonstrator

- Live feeds of video footage of the relevant laboratory and the mounted crystal under investigation;
- Still images (snap shots) of the crystal and the laboratory taken from the live video feed at certain time intervals. These images will also be able to be viewed in quick succession to form a fast forward version of the experiment.
- Lists of experimental data values for experiment times and other conditions such as temperature provided in numerical form;
- Live graphing of data values;
- CCD images of the X-ray diffraction pattern, where the position of the spots can be measured to determine the 3D structure under investigation;

Climate research demonstrator

- Sea Surface Temperature ('SST') data obtained from the AIMS/JCU collaboration; (Monash)
- Raw data in the form of plain text concerning climate information obtained by the Monash Climate Research Group from international sources; (Monash)
- Raw numerical data that relates to information such as position co-ordinates, coral bleaching and temperature obtained by the Monash Climate Research Group from international sources; (Monash)
- Data obtained from sensors that monitor the status of batteries that are providing power to the system; (James Cook)
- Raw data obtained from sensors concerning sea temperature, air temperature and air pressure; (James Cook)
- Images from a web cam positioned on the weather station where the sensor network is based. (James Cook)

At the time of writing this Interim Report, full details of the Climate Research demonstrator project at the University of Queensland were unavailable.

If all the criteria for protection are present, copyright may subsist in some of this data and images, perhaps as a literary work, a photograph or a cinematograph film. The fact that much of the data collected in the Crystallography and Climate research models is computer-generated means that the circumstances of creation would require examination to see if it is possible to identify one or more human authors.¹⁹ Possible authors could include those that have programmed the collection devices and/or those that operate the instruments (such as laboratory staff for crystallography experiments).

Examples of subject matter protected under copyright for demonstrator models

The crystallography demonstrator: The live video feeds, as well as the aggregation of the still images of the laboratory and crystal (if they are capable of being shown as a moving picture) may be protected under the Act as cinematographic films. The individual still images of the laboratory and crystal could be protected as photographs (artistic works) under the Act. The experimental data values could also be protected as literary works (which can include tables) while the graphical data may be protected as artistic works (which can include drawings – diagrams, maps, charts or plans).

The climate research demonstrator: All of the forms of data collected under this demonstrator could be protected as literary works, (if a human author is identified) as they are either in numerical or text form. The web cam images could be protected as cinematographic films if they are capable of being shown as a moving picture. On the other hand, if the web cam provides only 'snap shots', then these images could be protected as photographs.

The digital history demonstrator is not relevant here as it does not involve collection of data using instruments and other devices such as sensors.

4.2.2 Transfer and storage of data (DART SI packages)

The SI work packages are predominantly concerned with establishing mechanisms to allow the effective storage of data and the ability to exchange this data between systems. Hence, it is dealing with data that has been collected using instruments and other devices such as sensors (see discussion of DMQ packages above). It will also be dealing with other copyright subject matter that researchers deposit into a DART repository (for example, the types of materials that are created as part of the Digital History Model research may be involved).

In general, it seems that these work packages therefore involve reproduction of copyright material or substantial parts of that material. It may be possible that new original copyright subject matter is created using the raw data or existing copyright material. The following represents our understanding of the types of acts that may be performed with materials already deposited in the DART infrastructure as part of this process:

- Reproducing data stored within DART repositories. Various copies of the same data may be stored in different repositories, such as at each participating university.
- Regenerating simulation data. Work package SI6 concerns the development of computational services that allow simulation data to be regenerated dynamically. Instead of storing data from simulations in repositories, the DART project will store the input parameters for simulations and will rerun the simulation when required.
- Pre-processed/analysed data. SI7 will develop a pre-processing system that will refine, integrate and store real-time data streams from instruments and sensors in secondary storage. This data will be available for higher layers (later work package tools) to analyse, annotate and process.
- The repositories containing all of the raw forms of data as described under the DMQ section above, as well as pre-processed/analysed data. The primary (raw data) and secondary storage (pre-processed and

analysed data) repositories may be in the same physical machine. However, the repositories may be segmented within this storage medium. Data within these repositories will be held within discs and tapes.

It appears to us that these processes merely make copies of existing material. They do not appear to involve the creation of new copyright material. Hence the principal copyright issues relate to electronic databases and their protection as original literary works. It is not clear whether any of the storage functions could result in a depository within the DART infrastructure (as distinct from ARROW) acting as an 'archive' within the meaning of the Act.

Examples of copyright in subject matter within the SI work packages

The crystallography demonstrator: Under this demonstrator, pre-processing will involve converting the raw CCD X-ray images into 3-D representations (pictured below) of proteins using certain analysis software programs. The 3-D representations of proteins may be protected under copyright as an artistic work.

The database that stores crystallography data, Storage Resource Broker (SRB) will be available through a portlet, PGL. The SRB may qualify for copyright protection as a literary work being a compilation if it has sufficient originality. (s 10(1)) Originality in this context may be satisfied with the exercise of judgment and ingenuity in the arrangement of the database.

The climate research demonstrator: The Monash Climate Research group will be processing raw data through certain analytical programs to create climate models over particular periods of time and locations. These models are depicted as either graphs or 'maps' that show the co-ordinates and climate readings of certain areas. Nimrod/G and GriddLes may be used to re-simulate the model runs using particular input parameters. The input parameters could be stored in DART as well as, or instead of the graphs and maps. Therefore, it may be that the graphs and maps will be artistic works and that input parameters could be assessed to see whether they meet the requirements for a literary work. As with all copyright subsistence in works, it is essential to identify a human author. The repositories that hold all of this information (if the information is in fact held in any DART repositories) could also be protected as literary works being original compilations.

☛ TIP

Adequate security measures must protect against unauthorised interference with copyright material while it is being transferred and stored.

4.2.3 The submission of data and results by researchers into repositories (CR packages)

The nature of the information that is of interest to these work packages is likely to include the following:

1. Data collected from interview partners and focus group meetings. This data will be in the form of tapes, transcripts, text within a final report, and questionnaires (work package CR1);
2. Historical and other documents from personal repositories;
3. Datasets and other documents (for example, published documents) that are deposited into secondary repositories;
4. The above two forms of data that also have Creative Commons and Science Commons licences attached; and
5. Metadata, which is data about data. Metadata will be used to identify data for the purposes of storage, discovery and transfer within storage systems.

The deposit of copyright subject matter into DART repositories as well as making it available on-line or transmitting it electronically amount to the exercise of the exclusive rights of the copyright owner. For example, the digitisation of analogue print-based or artistic works will be regarded as 'reproducing the work in a material form' (s 31(1)). Reproduction under the Act includes converting a work from a hard copy into electronic form and vice versa (s 21(1A)). Furthermore, the digitisation of audio-visual items (film or recording) will be seen as 'making a copy' of the audio-visual item (ss 85(1), 86(1)). Even more importantly for the DART project, making digitised content available over the Internet, such as through websites, will be considered 'communication to the public' and may even be 'publication' of a work (ss 31(1), 85(1), 86(1)).²⁰

The critical issues that arise here relate to identifying the legal rights in materials which parties contribute to e-Research so that all necessary licences are obtained to enable the research collaborations to proceed efficiently. Difficulties that may arise include identifying whether copyright subsists, ownership of copyright and establishing appropriate licensing regimes.

Example of subject matter protected under copyright within CR work packages

Digital History demonstrator: Both projects in the Digital History demonstrator involve the deposit of various forms of historical data into DART repositories. This includes text (literary works), videos (films), photos (artistic works) and sound recordings. As this material may come from a number of historical sources it may not always be easy to identify the author or who owns the copyright. It will be important to identify not only that copyright subsists in the relevant work but that the necessary permission has been obtained from the copyright owners. For example, the makers of video footage submitted by the various projects will be the individual/s that undertook the arrangements necessary to make the video (s 22(4) in regards to films). This is normally the producer of a film, but in this research context it might be a combination of the person shooting the video, the producer and/or the interviewer. Another example could be a sound recording of live performances by aboriginal peoples or women at gatherings. The owner of copyright in the recording now vests in both the owner of the record and the performers themselves. (s 22(3A), (3B))

Other work packages within this DART project are considering appropriate licensing regimes for the e-Research environment. The Content and Rights Work package CR2 has the objective of reducing barriers to content acquisition by providing more rights-assignment options for non-science researchers. The Content and Rights Work Package CR3 has the objective of reducing barriers to content acquisition by providing more rights options for science researchers. Both groups are investigating the application of Creative Commons and Science Commons work to this e-Research environment.²¹

Contractual issues that arise from collaborative research of the nature envisaged by the DART project will be complex. There has already been some preliminary investigation of a number of the broad issues by other legal researchers. For example, in September 2003, Paul David and Michael Spence, from the Oxford Internet Institute (OII), released the final report of a JISC-supported project entitled, 'Towards institutional infrastructures for e-Science: the scope of the challenge'. The report concluded that the contractual issues were sufficiently complex to require the establishment of a new independent public body. The authors proposed that such a body would be needed to 'guide, oversee and disseminate the work of producing, maintaining, evaluating and updating standard contractual clauses, those being the constituent elements from which formal agreements may be more readily fashioned by the parties undertaking particular 'Grid-enabled' collaborations in science and engineering research'.²²

4.2.4 Annotation and assessment of research data (AA work packages)

The AA work packages will provide users with the ability to annotate subject matter that has been deposited into DART repositories. Furthermore, these work packages will also allow users to work collaboratively to edit digital objects and contribute to wikis. This means that users will be able to alter

material in which copyright subsists in ways that change that material and may result in a new copyright work or other subject matter. Those new works may then become either works of joint authorship (when all the contributions merge) or the separate annotations may constitute a separate copyright work. The ability to annotate means that the nature of the subject matter may be constantly changing.

Accordingly, the following forms of information may be subject to copyright:

- Annotations and contributions made to research data, reports and publications within the DART repositories;
- Collaborative works where real time annotations are made of digital objects such as images, videos and 3-D objects; and
- Hosted wikis that are linked to research data repositories.

In particular, DART will provide users with the collaborative annotation tool 'Vannotea', which allows text, images, web pages and threaded discussions (for example, entries of questions and answers) to be attached to digital objects. This tool also allows users to search for certain annotations. Furthermore, Vannotea can be used by parties in a collaboration to communicate through an online conference room, where each user's actions in relation to digital objects can be recorded and seen simultaneously by other participants. Vannotea also includes a web browser that can be used to access existing audio-visual archives.

The principal issues that arise as a consequence of the annotations process are likely to be:

1. to identify whether copyright subsists in the original work that is the subject of subsequent annotation;
2. to identify the relevant copyright work or other subject matter that arises through the process of annotation from time to time;
3. to identify who are its authors;
4. to identify who are its owners;
5. to identify what uses may be made of this material.

Some method of tracking the various iterations of works and the relevant authors might be necessary. For example, when the research collaboration results in a patentable invention, it will be important to identify the persons who supplied the inventive concept. The issues concerning patentable inventions and the possible commercial value of some of the research

outcomes that arise from e-Research collaborations in general are not developed in this Interim Report.

Those who make annotations to digital objects may be authors of the discrete matter that they have included. However, the individual who created the original digital object would remain an author of that object. While the authors of annotations may be the owners of copyright in what they create, this will depend upon any contractual arrangements that might alter the initial vesting of ownership in the author.

At this stage the nature of annotations is not entirely clear to us. It will be necessary to devise some precautions to remove the risk that the process of annotation could result in altering the work in a way that would infringe the moral rights of the author without justification. Those that make annotations should also be careful that they do not attach items that could make them liable for defamation. Liability of those involved in e-Research for defamatory statements may be explored further in the Final Report if feedback from the Interim Report indicates that this is desirable.

It will be necessary to design collaborative agreements between the various institutions who have staff, and possibly students, involved in e-Research collaboration that deal with, among other things, ownership of copyright material that is created in these circumstances as well as the rights that all parties can exercise over this material. It may be difficult in some circumstances, and may be undesirable, to rely upon unravelling the various separate contributions to what may become a final work that is to be published.

The complexities that may arise with deciding ownership of the copyright subject matter that is created using the DART infrastructure, and the manner in which rights are to be allocated, are still not clear to us. They will unfold as the details of specific research become evident. It is not clear to us whether the work being conducted in work packages CR2 and CR3 or as part of the Legal Protocols for Copyright Management: Facilitating Open Access to Research at the National and International Levels project will address and resolve these issues.²³

As annotations and contributions may have their own copyright protection, users of this annotated material under the DART project will need reassurance that they do not use the subject matter in a way that infringes copyright when they engage in collaborative research in ways for which DART (and ARCHER) is to be designed. It is not clear at this stage who can gain access to any of the data or documentation that will be deposited in a DART

repository for use in collaborative research. The collaboration agreement can address these issues if these rights of access are limited to the researchers themselves. We assume this limitation for the purposes of this Work Package. If broader access is envisaged, the conditions of access will require attention at a future date. Again, it is not clear whether the work being conducted in work packages CR2 and CR3 or under the Legal Protocols for Copyright Management will address and resolve these issues.

Examples of annotation and contribution issues raised by demonstrator models

Crystallography demonstrator: Crystallography researchers will be able to annotate one another's work using DART annotation tools. For example, textual annotations can be attached to specific sections of a 3-D representation of a protein structure by different researchers. These annotations may be protected as literary works, where the author is the individual that made the annotation. However, the original author of the 3-D image (if there is a human author) and the corresponding owner will still have rights to the original image. The image along with the annotations could be protected as an artistic work, which can include items such as maps, graphs or drawings. If the annotations are a separate literary work, the resulting annotated digital object could be a work of co-authorship, where the co-authors include the person that created the 3-D image and the individual who made the annotations.

Digital History demonstrator: Vannotea could be used by all three projects under the Digital History demonstrator. This collaborative annotation tool could be used to annotate video footage of interviews under the Gugu Badhun digital history project, footage from the Women on Farms project and the images from the Western Cape Community Project. Those that make annotations will have to ensure that they consider the moral rights of the authors of the original digital objects. Furthermore, while individual annotators may have authorship over their distinct annotations, if the annotations are made via collaborative contributions within a conference room and remain distinct from each other, the resulting work may be a work of co-authorship. Once the contributions merge in a way that they are no longer separate, the work would be a work of joint authorship.

4.2.5 Discovery and Access (DA work packages)

The DA work packages aim to provide users with tools that allow the discovery, sharing and re-use of information, as well as allowing depositors to control access to their material. The demonstrator models restrict the users to members of the respective collaborative research projects. However, it is likely that this e-Research infrastructure will be designed so that third parties may obtain access upon agreed terms to stored materials.

Repositories of materials are likely to contain copyright subject matter and have separate copyright protection as a literary work being a compilation.

These repositories may be created in the conduct of a particular research collaboration or may be existing databases held at participating institutions. For example, this may arise in the context of the Digital History demonstrator if the National Library of Australia's repository and the Museum Victoria's collection are linked into the DART infrastructure. However, at this stage, the precise involvement the DART project has in relation to each digital history demonstrator is not known. In particular, there are no details as to how each demonstrator will utilise DART annotation and collaboration tools, or whether the DART project will provide an interface for searching and retrieving stored data.

It is also necessary for precautions to be designed to ensure that there is no conduct that could amount to an authorisation for users to undertake any infringing acts that have not been authorised by the copyright owner.

Examples of discovery and access issues raised by demonstrator models

Digital History demonstrator: The Women on Farms website is a part of the Museum of Victoria's collection. Museum of Victoria wishes to encourage the use and examination of the resources within the site. However, the material is still subject to copyright restrictions. According to the website, the material available through the website (including sub-sites and other Museum material) can only be for personal use and cannot be copied, re-distributed, re-sold, framed or otherwise used without written permission from the Museum and/or from the original source (for example, the person that submitted the information). The material can be saved or printed for private research, while other uses also need prior permission. Other researchers who will be using the information will be those from the Women on Farms community, University of Otago on Rural Studies, Farming and Geography, and Monash University's Faculty of Arts and IT. As DART will be providing storage to archive this material, it will have to ensure that proper discovery and access mechanisms are in place that comply with the requirements for the Museum of Victoria, the access requirements of the other research participants and the protection requirements for copyright authors and owners.

4.3 PROTECTION OF CONFIDENTIAL INFORMATION: THE EQUITABLE DOCTRINE OF BREACH OF CONFIDENCE

It is possible to protect confidential information from unauthorized use or disclosure through the use of security measures, but also by imposing legal obligations of confidentiality upon the recipient. These obligations can be created through express or implied terms in contracts or may arise under the equitable action for breach of confidence. Generally, it is the person who is owed the duty of confidence or duty of good faith who can sue for infringement of the duty.

There are two particular areas in which it might be necessary to impose some limits on access to information that arises in the course of research projects. The first is where researchers collect personal and sacred information, including in relation to information concerning indigenous people and cultures. The second is where the information may have commercial value that would be destroyed by premature open disclosure.

When parties are in a contractual relationship they may be subject to express or implied obligations of confidentiality. It is important to read carefully the terms of any contract to determine what information is confidential and for what purposes it can be used or disclosed. The terms of a contract which expressly deals with issues of confidentiality should at least contain:

- A definition of the relevant confidential information;
- The recipient's obligations in regards to the information (such as permitted uses); and
- Details of the consequences which will flow if the recipient does not comply with these obligations.

In some cases contractual obligations to treat information as confidential may fail to achieve their required purpose.²⁴ Where there is no express obligation to treat information as confidential, or where the express obligation is unenforceable, it may be possible to imply an obligation from the circumstances.

Alternatively, an obligation may arise under the equitable doctrine of breach of confidence. There are many occasions where a person will want to communicate information to another in confidence on the understanding that the information is not further disseminated or used without consent. An equitable obligation of confidence arises without the need for a contractual relationship to exist between the provider and recipient of the confidential information.

The range of information that may be protected is extremely wide and extends to protect personal information, government secrets, business information and trade secrets, and a range of other ideas. Confidential information given by citizens to governments and their departments and agencies will also be protected. The information must have some significance in the sense that the preservation of its confidentiality or secrecy is of substantial concern to the plaintiff.

In Australia, four elements have to be met to establish an action for breach of confidence.²⁵ These are to:

- (a) identify with specificity, and not merely in global terms, that which is said to be the information in question;
- (b) show that the information has the necessary quality of confidentiality (and is not, for example, common or public knowledge);
- (c) show that the information was received by the defendant in such circumstances as to import an obligation of confidence; and
- (d) show that there is actual or threatened misuse of that information without the consent of the applicant.

It may also be that some element of detriment must be established, but this is not clear.

4.3.1 Identification of the Information

To **obtain protection** for the information under the action of breach of confidence, the applicant must identify clearly the information being relied upon in an action of breach of confidence.

4.3.2 Quality of Confidence

Information will not be protected unless it has the necessary quality of confidence. There can be no breach of confidence in revealing to others something that is already public property or public knowledge.²⁶ Absolute secrecy is not required.

4.3.3 Circumstances that Import an Obligation of Confidence

The third requirement is that the circumstances under which the information was received must 'import an obligation of confidence'. In this case, the principal question is whether 'any reasonable man standing in the shoes of the recipient of the information would have realised that the information was being given to him in confidence'.²⁷

4.3.4 Misuse of Information

If the information which possesses the necessary quality of confidence is disclosed or received in circumstances that impose an obligation of confidence, the recipient will breach this obligation when he or she uses or discloses the information or threatens to do so, in ways that were not permitted. There is no requirement for this use or disclosure to be deliberate or for there to be 'conscious plagiarism'.²⁸ However, the person must be aware (or have reason to be aware) at some stage of the confidential character of the information.²⁹ Third parties who receive or use information supplied by someone acting in breach of their duty of confidence can also be made subject to injunctions (court orders) which prohibit the use of the information.

4.3.5 Detriment

It is not clear whether an applicant must show that she has suffered detriment as a result of the breach of confidence. However, even if detriment is required, it may be simple to satisfy. For example, in personal matters, it may be enough that a person will suffer sufficient detriment where disclosure of information relating to his affairs has exposed him to public discussion and criticism. It may also be enough to merely suffer an unwanted disclosure.

4.3.6 Defences

Defences to an action for breach of confidence may apply for example where there is some just cause or excuse for disclosing the information (for example, where it is in public interest because it discloses some serious wrongdoing) or where there was some legal compulsion for disclosure.

4.4 CONFIDENTIALITY ISSUES ARISING AT SPECIFIC STAGES OF THE E-RESEARCH PROCESS

4.4.1 Collection of identifiable personal information via remote instruments (DART DMQ packages)

The raw data collected by sensors and/or instruments for the crystallography and climatology demonstrators as referred to under the discussion for copyright protection may also be protected as confidential information. This information includes:

- video images (live feed and compiled images – crystallography and climatology);
- still images (crystallography and climatology);
- CCD images (crystallography);
- experimental data values (crystallography and climatology); and
- graphical data (crystallography).

Protection of information will depend upon whether it is subject to confidentiality under contract or equitable principles.

It is likely that laboratory staff would be under express or implied obligations to treat the information as confidential arising from their contracts of employment. In the absence of contractual obligations, the equitable principles outlined above may be applicable. In the early stages of the research process, it is likely that all forms of raw data results will be kept confidential among the research collaborators. Thus, to a reasonable person, the information may have the quality of confidence. The information will only be public knowledge once it is made available to others without any restriction on what they may do with the information. Furthermore, in regards to the obligations of laboratory employees and others who receive this information as they collect it from instruments and sensors, a lot will depend upon the circumstances in which they do this work. It is arguable that the reasonable person would understand that sensitive research results must be kept secret until they have been analysed and the results published.

Example of collection issues raised by a demonstrator project

The crystallography demonstrator: Those that submit their crystals to the crystallography laboratory to obtain experimental results may wish to have the results kept confidential. In this event, it is preferable to make express reference to the nature and scope of obligations of confidentiality in a contract rather than to rely upon the equitable doctrine of breach of confidence or upon implied contractual terms.

4.4.2 Transfer and storage of data (DART SI packages)

When data is transferred and stored in various repositories, any identifiable confidential information will have to be kept secret. Confidentiality can be maintained through the adoption of security mechanisms that are discussed in Chapter 6.

4.4.3 The submission of data and results by researchers into repositories (CR packages)

This aspect of the project is more likely to involve the collection of data that may contain confidential information:

- Information obtained from research subjects in relation to their practices and views on research;
- Information obtained from researchers in relation to establishing ways to improve their information management practices;
- Historical data and other data from personal repositories; and
- Digital objects that are subject to Creative Commons and Science Commons licences

Information obtained from research subjects

Where confidential information is obtained from research subjects that participate in DART studies, the researchers must be aware of the need to ensure that confidences are maintained. In practice, these obligations will be regulated by Human Research Ethics Committees ('HRECs'), who only approve proposed research projects where they are satisfied that confidentiality (as well as other aspects such as privacy) of subjects is maintained.

Information relating to information management practices

DART researchers may collect or use data that contains confidential information when they establish information management practices in research groups. Therefore, they need to be aware of the circumstances in which they may become subject to a contractual or equitable duty of confidence to keep data secret. Those to whom they owe a duty of confidence may be members of the research group, or a third party who has given the group the information.

Historical data and other data from personal repositories

Those that place their research data into DART repositories will have to satisfy themselves that this action does not breach any duty of confidence they owe to someone else. It may be advisable for DART to incorporate some form of warning to alert researchers to the need to check that their actions will not breach a confidence before they deposit data. Preferably, the conditions for depositing information into DART repositories should deal with the issues that surround use and disclosure of confidential information in breach of confidence.

←TIP

Contracts that govern the use of the DART infrastructure should take into account the possibility that some information is subject to obligations of confidence.

4.4.4 Annotation and assessment of research data (AA work packages)

The following forms of data in DART may have annotations or contributions attached that contain confidential information:

- Research data, metadata, reports and publications within the DART repositories;
- Collaborative works where real time annotations are made of digital objects such as images, videos and 3-D objects; and
- Hosted wikis that are linked to research data repositories.

As with all forms of confidential information, the contracts that govern the use and operation of the DART infrastructure must consider all aspects of storage, use or disclosure of confidential information.

Examples of annotation issues raised by demonstrator projects

The crystallography demonstrator: DART will allow researchers to annotate 3-D protein structures. These annotations may contain confidential information, such as an analysis of results (research information) and information about those involved in the research process (personal information). Proper security mechanisms are necessary to protect this information from unauthorised use or disclosure.

The climatology demonstrator: Climatology researchers or reviewers will be able to annotate results that may include maps of climatology readings and sensor data. These annotations may also include researchers' analysis of readings and their identities. In relation to collaborative works, annotations may include correspondence between group members that may include sensitive research data and personal information about participants. This information will need to be protected within DART repositories against unauthorised use or disclosure.

The digital history demonstrator: DART will allow those involved in the Women on Farms demonstrator to annotate data, such as photographs and stories. It is possible that some of these annotations may contain information of a confidential nature.

4.4.5 Discovery and Access (DA work packages)

This aspect of DART aims to improve the use of DART repositories by providing end-user control over access. (discussed in Chapter 3). Therefore, depositors will need appropriate technology to maintain the confidentiality through imposition of controls on who can access that information and how they can use or disclose it. Without these controls, this information will lose its 'quality of confidence' when it becomes accessible to users without restriction.

DART may also use other discovery services, such as the national research discovery service hosted by the National Library of Australia. Where information is available through these services, DART will also have to ensure that the confidentiality of information is suitably protected. DART could establish agreements with these services to establish responsibility for information protection.

Examples of discovery and access issues raised by demonstrator projects

The crystallography demonstrator: Researchers will usually wish to restrict access to their results prior to publication. Therefore, access to data such as CCD images, video images, 3-D structures and any annotations or collaborative notes may need to be restricted for these earlier stages. Therefore, DART should ensure that there are appropriate security measures in place for owners of information to use.

The climatology demonstrator: Those conducting climatology research may want their data such as sensor readings and climatology maps to be kept confidential until publication. Thus, DART will have to provide owners with the appropriate security mechanisms to avoid any breaches of confidentiality that may arise through unintentional disclosure.

The digital history demonstrator: In regards to the Women on Farms Project, women may not want certain information to be disclosed, such as their names and/or contact details. Therefore, if this data is to be deposited in DART, there must be secure ways in which to protect the information from unauthorised disclosure or use.

Figure 4.1 - Determining subsistence of copyright in an item

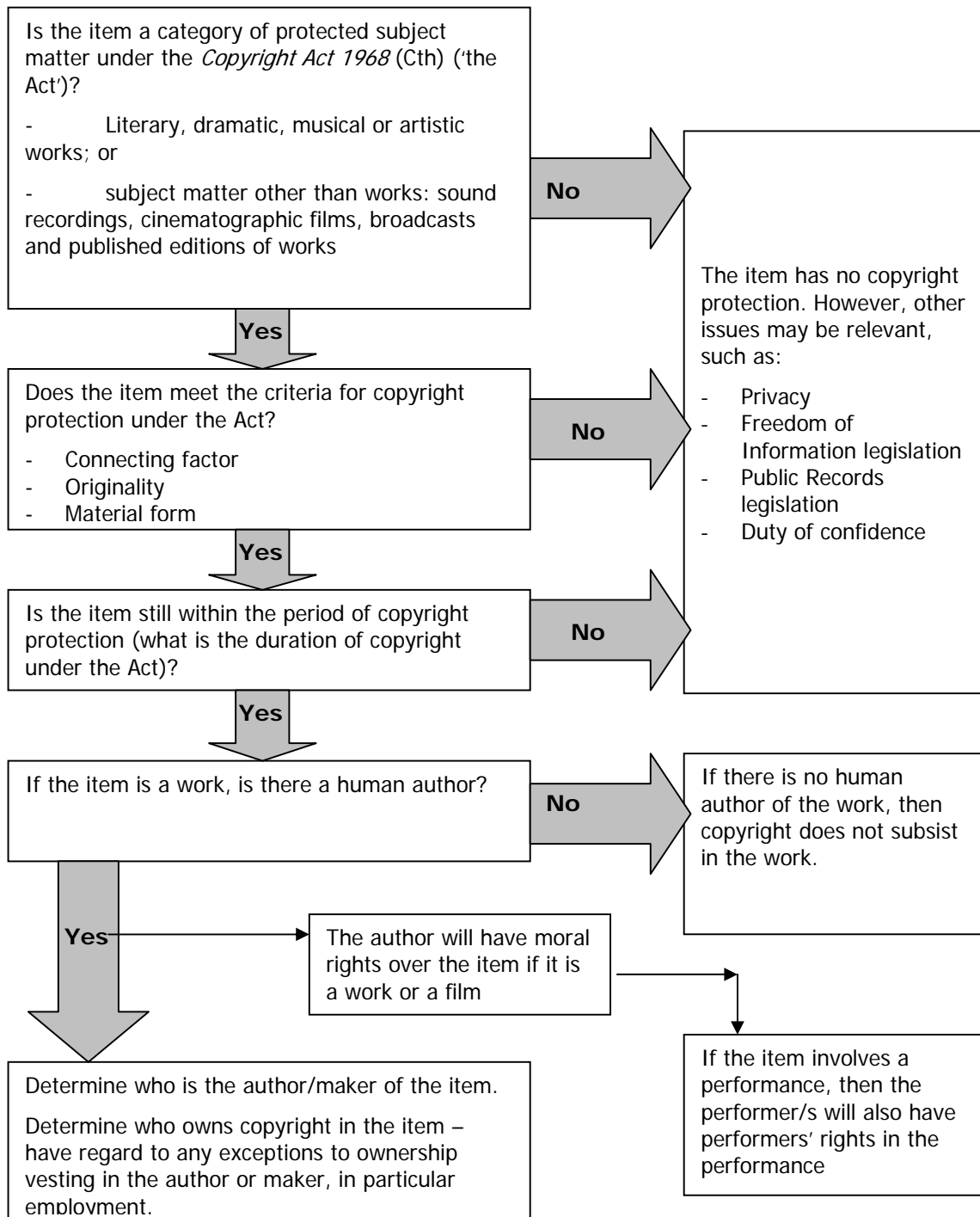
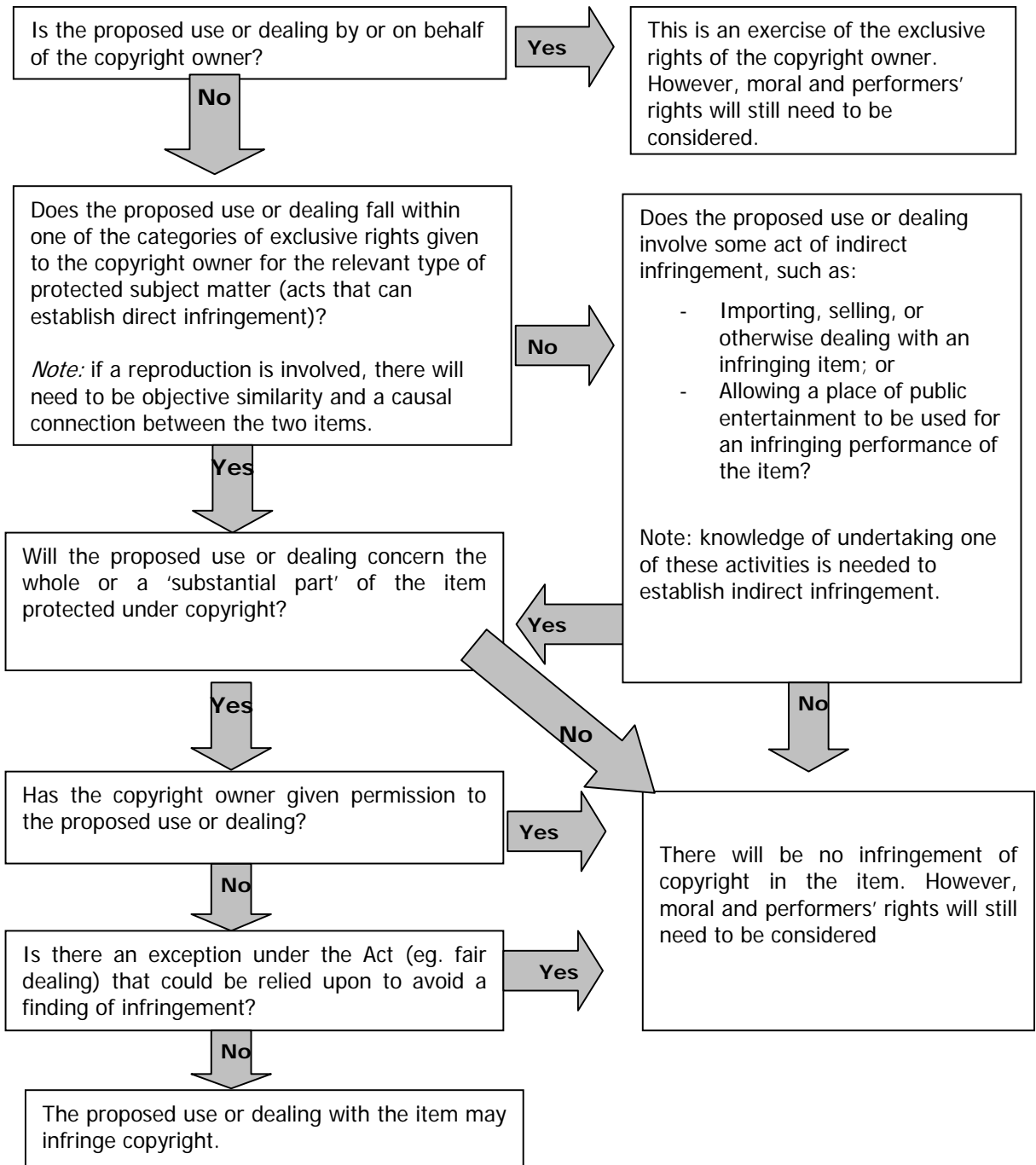


Figure 4.2 - Determining whether a proposed use or dealing with an item will be an infringement of copyright



4.5 PROTECTION OF CONFIDENTIAL INFORMATION: THE EQUITABLE DOCTRINE OF BREACH OF CONFIDENCE

An alternative form of protection for information is provided via legal obligations to keep information confidential. These can be created through terms in contracts or may arise via the equitable action for breach of confidence. Generally, it is the person who 'owns' the information, or is 'owed' the duty of confidence, that can bring an action for breach of confidence.

Why is the protection of confidential information important?

The duty of confidence is important because:

While security measures can be put in place to prevent unauthorised persons from accessing information, the duty of confidence prevents persons who already have the information from misusing it.

Its key role in the context of research is in protecting the value of information that may be commercially exploited through avenues such as patents or contracts.

It can also be used to protect personal and sacred information, including in relation to information concerning indigenous people and cultures.

a. Contractual Duty of Confidence

The use and disclosure of information is governed by contract if there is a contractual relationship between parties which regulates the status of information exchanged by them or the disclosure of information generated in the course of obligations arising under the contract. A duty of confidentiality may arise through express or implied terms of a contract.

It is important to read carefully the terms of any contract to determine what information is confidential and for what purposes it can be used or disclosed. The terms of a contract which expressly deals with issues of confidentiality should at least contain:

- A definition of the relevant confidential information;
- The recipient's obligations in regards to the information (such as permitted uses); and

- Details of the consequences which will flow if the recipient does not comply with these obligations.

To the extent that this information is not clearly spelt out it will need to be determined by way of implication.

In some cases contractual obligations to treat information as confidential may fail to achieve their required purpose. For example, in the case of *Maggbury Pty Ltd v Gisma Pty Ltd*,³⁰ it was held that there was no contractual duty of confidence because the relevant information had already entered the public domain (ie, it was already public knowledge). Likewise, contractual obligations to treat information as confidential may be overridden by statutory requirements for disclosure.

Where the obligation to treat information as confidential is not spelt out expressly within a contract, it may be implied from the circumstances (including past practice). Alternatively, it may arise via the equitable duty of confidence.

b. Equitable Duty of Confidence

An equitable obligation of confidence does not require any contractual obligations between the person who provides information and the person to whom it is given, although a contractual relationship does not preclude its existence. It will arise where confidential information 'owned' by one person is communicated or obtained by another under circumstances that give rise to an obligation to keep the information confidential.³¹

In Australia, four elements have to be met to establish an action for breach of confidence.³² These are to:

- (a) identify with specificity, and not merely in global terms, that which is said to be the information in question;
- (b) show that the information has the necessary quality of confidentiality (and is not, for example, common or public knowledge);
- (c) show that the information was received by the defendant in such circumstances as to import an obligation of confidence; and
- (d) show that there is actual or threatened misuse of that information without the consent of the applicant.

4.5.1 Identification of the Information

To be able to sue for breach of confidence an applicant must be able to identify specifically (rather than in general terms) the information to which that duty relates.

The types of information that can be considered confidential includes:

- Commercially valuable information (such as research results or trade secrets);
- Other information acquired by a person in the context of their employment, including employment by a government agency; and
- Personal information, including traditional sacred or secret knowledge of indigenous people and private information.³³ Secret indigenous information has been protected from disclosure in two Australian cases. The first case concerned the publication of a book containing secret/sacred indigenous information,³⁴ while the second case concerned the selling of lantern slides that also contained secret/sacred information.³⁵

4.5.2 Quality of Confidence

Secondly, the information must have 'the necessary quality of confidence' and not be common or public knowledge. The information does not have to be absolutely confidential in the sense of being unknown by anyone else;³⁶ instead it must not be in the public domain,³⁷ for example by being disclosed in a publicly-available document (even without the consent of its 'owner').

In Australia, a 'reasonable man' test has been utilised to establish whether information possesses the required quality of confidence. This poses the question whether a person of ordinary intelligence in the circumstances, including the relationship of the parties, the nature of the information, and the circumstances of its communication, would recognise that the information is the property of the other person and not his own to do with what he likes.³⁸ Other considerations can include:

- The conduct of the confider;³⁹
- The extent to which the information is known;
- The measures taken to guard the information;
- The value of the information;
- The amount of money expended to protect the information; and

- The difficulty of properly acquiring or duplicating the information.⁴⁰

4.5.3 Circumstances that Import an Obligation of Confidence

The third requirement is that the circumstances under which the information was received must 'import an obligation of confidence'. In this case, the question is whether 'any reasonable man standing in the shoes of the recipient of the information would have realised that the information was being given to him in confidence'.⁴¹ Other considerations may include:⁴²

- The pre-existing relationship of the parties;
- Whether the information was supplied for consideration (ie, in return for some payment or benefit);
- Past practice;
- The sensitivity of the information;
- Whether the confider has any interest in the use of the information; and
- Whether the confidant was expressly warned against a particular disclosure or use.

4.5.4 Misuse of Information

The final requirement is that there must be actual or threatened misuse of the information without the consent of the confider. Unauthorised use is found where the recipient of confidential information discloses or uses the information beyond the purpose for which it was given. Consequently, what the information will be used or disclosed for must also be specifically identified.⁴³ It makes no difference whether the misuse is intentional, unintentional, subconscious or negligent.⁴⁴ Third parties who receive or use information supplied by someone acting in breach of their duty of confidence can also be made subject to injunctions (court orders) which prohibit the use of the information.⁴⁵

4.5.5 Defences

There are two possible defences to an action for breach of confidentiality. The first arises where there is some just cause or excuse for disclosing the information (for example, where it is in public interest because it discloses some serious wrongdoing).⁴⁶ The second defence arises where there was

some legal compulsion for disclosure (eg, where the information is obtained under a search warrant or is required to be disclosed under some statute).⁴⁷

4.5.6 Confidentiality issues arising at specific stages of the E-Research process

(i) Collection of identifiable personal information via remote instruments (DART DMQ packages)

The raw data collected by sensors and/or instruments for the crystallography and climatology demonstrators as referred to under the discussion for copyright protection may also be protected as confidential information. This information includes:

- video images (live feed and compiled images – crystallography and climatology);
- still images (crystallography and climatology);
- CCD images (crystallography);
- experimental data values (crystallography and climatology); and
- graphical data (crystallography).

Protection of the information will depend upon whether the raw data is subject to confidentiality under contract or equitable principles.

It is likely that laboratory staff would be under express or implied obligations to treat the information as confidential arising from their contracts of employment. In the absence of contractual obligations, the equitable principles outlined above may be applicable. In the early stages of the research process, it is likely that all forms of raw data results will be kept confidential among the research collaborators. Thus, to a reasonable person, the information may have the quality of confidence. The information will only be public knowledge once it is made available to others without any restriction on what they may do with the information. Furthermore, in regards to the obligations of laboratory employees and others who receive this information as they collect it from instruments and sensors, a lot will depend upon the circumstances in which they do this work. It is arguable that the reasonable person would understand that sensitive research results must be kept secret until they have been analysed and the results published.

Example of collection issues raised by a demonstrator project

The crystallography demonstrator: Those that submit their crystals to the crystallography laboratory to obtain experimental results may wish to have the results kept confidential. In this event, it is preferable to make express reference to the nature and scope of obligations of confidentiality in a contract rather than to rely upon the equitable doctrine of breach of confidence or upon implied contractual terms.

(ii) Transfer and storage of data (DART SI packages)

When data is transferred and stored in various repositories, any identifiable confidential information will have to be kept secret. Confidentiality can be maintained through the adoption of security mechanisms that are discussed in Chapter 8.

(iii) The submission of data and results by researchers into repositories (CR packages)

This aspect of the project will involve the collection of the following data that may contain confidential information:

- Information obtained from research subjects in relation to their practices and views on research;
- Information obtained from researchers in relation to establishing ways to improve their information management practices;
- Historical data and other data from personal repositories; and
- Digital objects that are subject to Creative Commons and Science Commons licences

Information obtained from research subjects

Where confidential information is obtained from research subjects that participate in DART studies, the researchers must ensure that the confidence is maintained. In practice, these obligations are regulated by Human Research Ethics Committees ('HRECs'), who only approve proposed research projects where they are satisfied that confidentiality (as well as other aspects such as privacy) of subjects is maintained.

Information relating to information management practices

DART researchers may collect or use data that contains confidential information when they establish information management practices in research groups. Therefore, they need to be aware of the circumstances in which they may become subject to a contractual or equitable duty of confidence to keep data secret. Those to whom they owe a duty of confidence may be members of the research group, or a third party who has given the group the information.

Historical data and other data from personal repositories

Those that place their research data into DART repositories will have to satisfy themselves that this action does not breach any duty of confidence they owe to someone else. It may be advisable for DART to incorporate some form of warning to alert researchers to the need to check that their actions will not breach a confidence before they deposit data. Preferably, the conditions for depositing information into DART repositories should deal with the issues that surround use and disclosure of confidential information in breach of confidence.

← TIP

Contracts that govern the use of the DART infrastructure should take into account the possibility that some information is subject to obligations of confidence.

(iv) Annotation and assessment of research data (AA work packages)

The following forms of data in DART may have annotations or contributions attached that contain confidential information:

- Research data, metadata, reports and publications within the DART repositories;
- Collaborative works where real time annotations are made of digital objects such as images, videos and 3-D objects; and
- Hosted wikis that are linked to research data repositories.

DART must ensure that annotations or contributions to these forms of data do not contain information where its use or disclosure may be in breach of a duty of confidence

As with all forms of confidential information, the contracts that govern the use and operation of the DART infrastructure must consider all aspects of storage, use or disclosure of confidential information.

Examples of annotation issues raised by demonstrator projects

The crystallography demonstrator: DART will allow researchers to annotate 3-D protein structures. These annotations may contain confidential information, such as an analysis of results (research information) and information about those involved in the research process (personal information). DART should ensure that proper security mechanisms are in place to protect this information from unauthorised use or disclosure.

The climatology demonstrator: Climatology researchers or reviewers will be able to annotate results that may include maps of climatology readings and sensor data. These annotations may also include researchers' analysis of readings and their identities. In relation to collaborative works, annotations may include correspondence between group members that may include sensitive research data and personal information about participants. This information will need to be protected within DART repositories against unauthorised use or disclosure.

The digital history demonstrator: DART will allow those involved in the Women on Farms demonstrator to annotate data, such as photographs and stories. These annotations may contain personal information about individuals, such as the names and addresses of those that have participated in Women on Farms gatherings. The consent of individuals that are subjects of confidential information may need to be obtained before information is used or disclosed within DART repositories.

(v) Discovery and Access (DA work packages)

This aspect of DART aims to improve the use of DART repositories by providing end-user control over access. (discussed in Chapter 4). Therefore, depositors will need appropriate technology to maintain the confidentiality through imposition of controls on who can access that information and how they can use or disclose it. Without these controls, this information will lose its 'quality of confidence' when it becomes accessible to users without restriction.

DART may also use other discovery services, such as the national research discovery service hosted by the National Library of Australia. Where information is available through these services, DART will also have to ensure

that the confidentiality of information is suitably protected. DART could establish agreements with these services to establish responsibility for information protection.

Examples of discovery and access issues raised by demonstrator projects

The crystallography demonstrator: Researchers will usually wish to restrict access to their results prior to publication. Therefore, access to data such as CCD images, video images, 3-D structures and any annotations or collaborative notes will have to be restricted for these earlier stages. Therefore, DART should ensure that there are appropriate security measures in place for owners of information to use.

The climatology demonstrator: Those conducting climatology research may want their data such as sensor readings and climatology maps to be kept confidential until publication. Thus, DART will have to provide owners with the appropriate security mechanisms to avoid any breaches of confidentiality that may arise through unintentional disclosure.

The digital history demonstrator: In regards to the Women on Farms Project, women may not want certain information to be disclosed, such as their names and/or contact details. Therefore, if this data is to be deposited in DART, there must be secure ways in which to protect the information from unauthorised disclosure or use.

ENDNOTES

¹ There is no shortage of sources from which greater detail is available. For example: Brian Fitzgerald et al, *Oak Law Report* (2006) <<http://www.oaklaw.qut.edu.au>> Ch 2 and 3; Staniforth Ricketson and Christopher Creswell, *The law of intellectual property: copyright, designs & confidential information* (2nd ed (rev), 1999-); Sam Ricketson and Megan Richardson, *Intellectual property: cases, materials and commentary* (3rd ed, 2005); Jill McKeough, Andrew Stewart and Philip Griffith, *Intellectual property in Australia* (3rd ed, 2004).

² *Copyright Act 1968* (Cth) s 32 (works), ss 89-92 (subject matter other than works).

³ HMSO, *Gowers Review of Intellectual Property* (2006) Executive Summary E.9 <http://www.hm-treasury.gov.uk/media/583/91/pbr06_gowers_report_755.pdf> contains a recommendation to propose a provision to the European Commission which would unlock material that was previously unusable.

⁴ Subsections 35(4), (5) and (6) must also not apply. The same presumption applies to each author in a work of joint authorship.

⁵ For example: *Express Newspapers Plc v Liverpool Daily Post and Echo Plc* [1985] FSR 306.

⁶ Copyright Law Review Committee, *Computer Software Protection* (1995) [13.11].

⁷ *Copyright, Designs and Patents Act 1988* (UK) s 9(3). A computer-generated work is defined as a work that is generated by computer in circumstances where there is no human author of a work: *Copyright, Designs and Patents Act 1988* (UK) s 178.

⁸ Copyright Law Review Committee *Computer Software Protection* (1995) [13.13A – 13.23]

⁹ Copyright Law Review Committee, *Simplification of the Copyright Act 1968, Part 2: Categorisation of Subject Matter and Exclusive Rights, and Other Issues*, 1999 [5.42 – 5.47].

¹⁰ A L Monotti with S Ricketson, *Universities and Intellectual Property: Ownership and Exploitation* (2003).

¹¹ Schedule 9 Part 2 (items 16-58) of the *US Free Trade Implementation Act 2004* (Cth) introduces performers' moral rights. These provisions are yet to commence.

¹² For works and subject matter other than works that are made or published by, or under the direction or control of, an international organisation: *Copyright Act 1968* (Cth), ss 187, 188.

¹³ *Ladbroke (Football) Ltd v William Hill (Football) Ltd* [1964] 1 All ER 465 at 469, per Lord Reid.

¹⁴ *Slessor LJ* at [1934] 1 Ch 593 at 607.

¹⁵ *Ladbroke (Football) Ltd v William Hill (Football) Ltd* [1964] 1 All ER 465 at 481, per Lord Pearce; *Data Access Corporation v Powerflex Services Pty Ltd* (1999) 202 CLR 1.

¹⁶ *TCN Channel Nine Pty Ltd v Network Ten Pty Ltd* [2005] FCAFC 57.

¹⁷ *TR Flanagan Smash Repairs Pty Ltd v Jones* (2000) 172 ALR 467.

¹⁸ Considerable work is being done in this area to assist the development of standard licences that are suitable for academic and research outputs. In 2005, DEST funded an investigation into 'a legal framework that supports open access to Australian academic and research outputs such as datasets, articles and electronic theses and dissertations.' The Oak Law Report was released on 28 September 2006: Brian Fitzgerald et al, *Oak Law Report* (2006) <<http://www.oaklaw.qut.edu.au>>.

¹⁹ See discussion of computer generated works in: Copyright Law Review Committee, *Computer Software Protection* (1995).

²⁰ Emily Hudson and Andrew T Kenyon, 'Copyright and Cultural Institutions: Guidelines for Digitisation', Melbourne Law School Legal Studies Research Paper No. 140 (2006) <<http://ssrn.com/abstract=881699>> 41.

²¹ Brian Fitzgerald et al, *Oak Law Report* (2006) <<http://www.oaklaw.qut.edu.au>>.

²² Paul A. David and Michael Spence, 'Towards institutional infrastructures for e-Science: the scope of the challenge', Oxford Internet Institute, Research Report No. 2, September 2003 (2003) <www.oii.ox.ac.uk/resources/publications/RR2.pdf> 11.

²³ In July 2006, the Minister for Education, Science and Training announced funding under the Systemic Infrastructure Initiative funding for a new project, *Legal Frameworks for e-Research*, which will extend and reinforce the work already being undertaken by the Legal Protocols for Copyright Management for Open Access project: The Hon Julie Bishop MP, *Media Centre* (2006) <<http://www.dest.gov.au/Ministers/Media/Bishop/2006/07/B001310706.asp>>.

²⁴ *Maggbury Pty Ltd v Hafele Australia Pty Ltd* (2001) 210 CLR 181.

²⁵ *Smith Kline & French Laboratories (Australia) Ltd v Secretary, Department of Community Services and Health* (1990) 17 IPR 545, per Gummow J.

²⁶ *Coco v A N Clark (Engineers) Ltd* [1969] RPC 41, 47; *Saltman Engineering Co Ltd v Campbell Engineering Co Ltd* [1963] 3 All ER 413, 415.

²⁷ *Coco v AN Clark (Engineers) Ltd* [1969] RPC 41 at 48, per Megarry J.

²⁸ *Seager v Copydex Ltd* [1967] 2 All ER 415, 418.

²⁹ *Talbot v General Television Corporation Pty Ltd* [1980] VR 224.

³⁰ [1999] QSC 4 (22 January 1999)

³¹ *Moorgate Tobacco Co Ltd v Philip Morris Ltd (No 2)* (1984) 156 CLR 414 at 437-8.

³² *Smith Kline & French Laboratories (Australia) Ltd v Secretary, Department of Community Services and Health* (1990) 17 IPR 545, per Gummow J.

³³ The World Intellectual Property Organisation is working in this area. See the report: WIPO, *Intellectual Property Needs and Expectations of Traditional Knowledge Holders*, WIPO Report on Fact-Finding Missions 1998-1999 (1999) <http://books.google.com/books?id=soLlz5TSW8MC&dq=Intellectual+Property+Needs+and+Expectations+of+Traditional+Knowledge+Holders&pg=PP1&ots=UuWLZO_ao4&sig=lg9heWjzqQSH60IPKX10BPa2Sb8&prev=http://www.google.com/search%3Fsourceid%3Dnavclient%26ie%3DU TF-8%26rls%3DHPAB,HPAB:2005-32.HPAB:en%26q%3DIntellectual%2BProperty%2BNeeds%2BAnd%2BExpectations%2Bof%2BTr additional%2BKnowledge%2Bholders&sa=X&oi=print&ct=result&cd=1>.

³⁴ *Foster v Mountford & Rigby Ltd* (1976) 14 ALR 71.

³⁵ *Pitjantjatjara Council Inc and Nganingu v Lowe and Bender* (unreported, Supreme Court of Victoria, Crockett J, 25 and 25 March 1982), discussed in: Ross Howie, 'Pitjantjatjara Council Inc and Peter Nganingu V John Lowe and Lyn Bender' [1982] *Aboriginal Law Bulletin* 30.

³⁶ *Coulthard v The State of South Australia, McKenzie v The State of South Australia, Champion v The State of South Australia* [1995] SASC 4927.

³⁷ *Saltman Engineering Co Ltd and Others v Campbell Engineering Co Ltd* [1963] 3 All ER 413, 415.

³⁸ *Deta Nominees Pty Ltd v Viscount Plastic Products Pty Ltd* [1979] VR 167 at 193, per Fullagar J.

³⁹ *Ansell Rubber Co Pty Ltd v Allied Rubber Industries Pty Ltd* [1967] VR 37.

⁴⁰ *Ansell Rubber Co Pty Ltd v Allied Rubber Industries Pty Ltd* [1967] VR 37 at 49-50.

⁴¹ *Coco v AN Clark (Engineers) Ltd* [1969] RPC 41 at 48, per Megarry J.

⁴² Full Federal Court in *Smith Kline & French Laboratories (Australia) Ltd v Secretary, Department of Community Services and Health* (1991) 20 IPR 643.

⁴³ *O'Brien v Komesaroff* (1982) 150 CLR 310; *Corrs Pavey Whiting & Byrne v Collector of Customs (Vic)* (1987) 74 ALR 428.

⁴⁴ *Seager v Copydex Ltd* [1967] 2 All ER 415. It is not clear whether detriment to the confider or owner of the information is required in determining liability for a breach of confidence. According

to Gummow J in *Smith Kline & French Laboratories (Australia) Ltd v Secretary, Department of Community Services and Health* (1990) 17 IPR 545 at 584, no detriment is required. However, Dean J in *Moorgate Tobacco Co Ltd v Philip Morris Ltd (No 2)* (1984) 156 CLR 414 at 438, refers to a need for the plaintiff to have a 'substantial concern'.

⁴⁵ This liability will arise upon actual or constructive notice of the breach, if the third party was unaware of the breach from the outset: *Fraser v Evans* [1969] 1 QB 349.

⁴⁶ There will be no breach where misconduct is disclosed to proper authorities in the public interest: *Gartside v Outram* (1856) 26 LJ Ch 113; *Attorney-General (UK) v Heinemann Publishers Australia Pty Ltd* (1988) 165 CLR 30.

⁴⁷ This may be required under statute or ordered by a court for litigation. However, the recipient or person or body receiving the information under legal compulsion may also be required to keep the information confidential: Full Federal Court in *Smith Kline & French Laboratories (Australia) Ltd v Secretary, Department of Community Services and Health* (1991) 20 IPR 643.

5 PRIVACY AND RELATED LAWS

There are a number of different regimes which govern information handling practices within Australian universities. These include information privacy and health records laws, anti-surveillance laws, Freedom of Information Acts and Archives/Public Records laws. The main focus of this chapter will be on privacy but the other laws will also be discussed to the extent that they are specifically relevant to information handling in the context of e-Research.

5.1 PRIVACY

5.1.1 Introduction

Privacy is inherently personal and is concerned with the desire to be separate or individual. It has been described as 'the condition of an individual when he is free from interference with his intimate personal interests by others'.¹

Although it has many different dimensions, those which are likely to be of most relevance to the DART project and e-Research more broadly are information privacy and privacy from surveillance.

Why is privacy important?

It is important because:

1. It is a necessary element of respect for the individual
2. It provides valuable protection from discrimination and
3. It offers a space for individual development and self expression

In the absence of privacy protection individuals are less likely to have confidence in sharing or making available their personal information.

This chapter will provide a discussion of the general legal principles which govern the protection of privacy in Australia. This will then be followed by an outline of the types of personal information that will be generated under each stage of the DART project and the legal constraints that will regulate the collection, storage, disclosure and use of this information.

5.1.2 Legal protection

Information privacy in Australia is protected via:

- Information privacy laws;
- Statutes which protect the secrecy of specific information (for example, tax records); and
- Statutes which prohibit specified surveillance activities.

It also receives some limited protection at common law.

5.1.3 Information privacy laws

(i) Coverage

The coverage of Australian information privacy laws is summarised in Table 7.1.

Commonwealth and Territory public sector agencies (including public universities) and public sector agencies in those States that have enacted information privacy and health records laws are required to comply with privacy principles in relation to personal information (as described below) collected and held by them.

Private sector organisations (including private universities and private bodies within universities) are regulated by a separate set of National Privacy Principles ('NPPs') in the *Privacy Act 1988* (Cth) (Commonwealth Act). An 'organisation' is defined in s 6C(1) as 'an individual, a corporation a partnership, and any other unincorporated association, or a trust'. Under section 6C(2), a legal person who acts in more than one capacity can be considered a different organisation for each role. For example, a person who is a trustee for various different trusts will be seen as a separate organisation for each trust.

(ii) Bodies excluded from the private sector provisions

Subject to a number of exceptions (including exceptions for organisations which provide health services or sell personal information), private sector provisions in the Commonwealth Act do not apply to small business operators (defined in s 6D as organisations with an annual turnover for the previous financial year of \$3,000,000 or less). The exclusion for small business operators is, however, subject to a number of important exceptions. For example, a body which is contracted service provider to the Commonwealth

government or which provides health services to individuals will not qualify for exemption irrespective of its annual turnover.

The private sector provisions also do not apply to the acts or practices of the bodies listed in s 7 or the acts and practices specified in ss 7B and 7C (including the activities of employers in relation to employee records, the activities of media organizations in relation to journalism activities, the activities of contractors under State contractors in relation their contracts and the political activities of political representatives).

(iii) Personal information

The definition of ‘personal information’ in s 6(1) of Commonwealth Act is reasonably typical. It refers to information or opinion, whether true or not ‘about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion’. Therefore, personal information can include information that does not identify the person by name if it includes other material that can be used to identify a person. Personal information may take the form of photographs or other visual images as well as writing and material stored in a database.

TABLE 5.1 - Australian information privacy laws

Jurisdiction	Legislation	Coverage	Privacy Principles
Commonwealth	<i>Privacy Act 1988</i> (Cth)	‘Agencies’ -see s 6(1)	Information Privacy Principles - s 14
		‘Organisations’ – see s 6C(1)	National Privacy Principles - Schedule 3
Australian Capital Territory	<i>Privacy Act 1988</i> (Cth) and <i>Government Service (Consequential Amendments) Act 1994</i> (ACT)	As above	As above
New South Wales	<i>Privacy and Personal Information Protection Act 1998</i> (NSW)	‘Public sector agencies’ – see s 3(1)	Information Privacy Principles – Part 2, Division 1
Northern Territory	<i>Information Act 2002</i> (NT)	‘Public sector agencies’ – see s 5(1)	Information Privacy Principles –s 65 and Schedule
Queensland	No information privacy legislation	Public sector agencies must follow an administrative	-

Jurisdiction	Legislation	Coverage	Privacy Principles
		scheme based on the principles in the Cth Act	
South Australia	No information privacy legislation	A Cabinet Administrative Instruction requires public sector bodies to comply with a set of Information Privacy Principles	-
Tasmania	<i>Personal Information Protection Act 2004</i> (Tas)	'Personal information custodians' – see s 3	Personal information protection principles – s 16, Schedule
Victoria	<i>Information Privacy Act 2000</i> (Vic)	'Public sector organisations' – see s 9(1)	Information Privacy Principles Schedule 1
Western Australia	No information privacy legislation	-	-

(iv) The information privacy principles

The information privacy laws operate by requiring compliance with sets of information privacy principles which regulate the collection, storage, use, disclosure and accessibility of identifiable personal records. Those principles, which are listed in Table 5.3, are designed to give individuals a greater level of control over their own personal information.

The principles relating to collection ('collection principles') require information must be collected only by fair and lawful means and for purposes related to the functions or activity of the collecting organisation. They also operate to ensure that individuals whose identifiable information is collected are made aware of what has been collected and that they are informed about the purposes of that collection and the persons to whom that information is likely to be passed on. Most Acts also require that information must as far as possible be collected directly, rather than indirectly via other people or organisations ('direct collection').

The principles governing storage regulate what must be done with information collected and consist of three elements:

1. Information quality provisions which require that personal information collected and held must be relevant, up to date and complete, having regard to the purposes for which it is used;
2. Security principles which require the adoption of reasonable measures to safeguard personal information held against unauthorised access, disclosure, loss, improper modification and other misuse; and
3. Non-retention principles which require the destruction or de-identification of personal information when it is no longer required for the purposes for which it was collected.

The principles concerning access and amendment provide individuals with the right to access to their own personal records and to request the amendment of any information which is inaccurate, misleading, out of date or irrelevant to the purposes for which it was collected. They are supplemented by openness principles which require record-keepers to make available information (for example, in the form of a privacy statement) to assist in the exercise of privacy rights, including the rights of access.

Finally, principles that impose use and disclosure limitations require that:

- Uses of personal information collected must be confined to purposes to which the information is relevant;
- Uses of personal information collected must be confined to the purposes for which the information was collected; and
- Disclosures must be confined to persons and bodies to whom the information subject could reasonably have expected the information to be passed.

They do not preclude uses and disclosures that are made with the consent of the person concerned, where the use or disclosure is required or authorised by law (including under freedom of information or public records legislation, which is discussed further below), or where it is required for law enforcement purposes.

Additional principles that also exist in some of the Acts are as follows:

- Anonymity principles which require that individuals, where practicable, should be able to enter into transactions on an anonymous basis;
- Principles which limit the use of unique identifiers (which are strings of characters, usually numbers – for example a tax file number - used to identify particular individual) assigned by public sector agencies;

- Transborder dataflow principles which restrict the transfer of personal information to other jurisdictions in circumstance where it will lack equivalent privacy protection; and
- Principles which impose additional limitations in respect of more sensitive categories of personal information. Sensitive information includes information concerning a person's political opinions, racial origin, religious or philosophical beliefs, health or sexual activities and trade union memberships.

(v) Oversight and enforcement of privacy requirements

The legislation is subject to oversight by Privacy Commissioners and Information Commissioners as set out in Table 5.4. Privacy complaints are generally resolved via a process of conciliation but breaches may result in requirements to pay compensation and to take appropriate measures to mitigate any harm to an individual (for example, the removal of material from a database).

Except in the case of private sector provisions and the *Information Act 2002* (NT), access and amendment rights are exercised and enforced via Freedom of Information legislation (as outlined further below).

Table 5.2 - Relevant exceptions to 'personal information'

Exception	Legislation	Application examples
Generally available publications and other similar information	<i>Privacy Act 1988</i> (Cth), s 6(1)	The Commonwealth Act defines 'generally available information' as 'a magazine, book, newspaper or other publication (however published) that is or will be generally available to members of the public'
	<i>Privacy and Personal Information Protection Act 1988</i> (NSW), s 4(3)	The New South Wales Act excludes from its operation 'information about an individual that is contained in a publicly available publication'
	<i>Information Act 2002</i> (NT), s 68(1)(a)	In the Northern Territory, the IPPs (except for IPP 1 and 3) do not apply to information that 'is published in a publication (which may be an electronic publication) generally available to members of the public'

Exception	Legislation	Application examples
	<i>Personal Information Protection Act 2004</i> (Tas), ss 3, 8	In Tasmania, the Act does not apply to 'public information', which means personal information that is 'contained in a publicly available record or publication', or 'taken to be public information under any Act
	<i>Information Privacy Act 2000</i> (Vic), ss 3 (definition), 11(1)(a)	The Victorian Act defines 'generally available publication' as 'a publication (whether in paper or electronic form) that is generally available to members of the public and includes information held on a public register'
Information about deceased persons	<i>Privacy Act 1988</i> (Cth), s 6(1) ('individual')	The Commonwealth Act only applies to people that are alive
	<i>Privacy and Personal Information Protection Act 1988</i> (NSW), s 4(3)	'Personal information' under the New South Wales Act does not include 'information about an individual who has been dead for more than 30 years'
	<i>Information Act 2002</i> (NT), s 4	Under the Northern Territory Act, the definition of 'person' includes a person who has passed away within the last five years
	<i>Personal Information Protection Act 2004</i> (Tas), s 3	Under the Tasmanian Act, 'personal information' does not include information about an individual who has been dead for more than twenty five years
	<i>Information Privacy Act 2000</i> (Vic), s3	The Victorian Act only applies to people that are alive ('individual' means a 'natural person')
Information held in libraries, art galleries or museums	<i>Privacy Act 1988</i> (Cth), s 6(1)	In the Commonwealth Act, the term 'record' does not include 'anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition'
	<i>Information Act 2002</i> (NT), s 68(1)(c), (e)	The NT IPPs (except for IPP 1 and 3) do not apply to information that 'is an archive available to the public under Part 9, Division 4 (Managing archives)' or 'in a

Exception	Legislation	Application examples
		collection of a library, art gallery or museum if the collection is on public exhibition or is available to the public for reference or study purposes'
	<i>Information Privacy Act 2000</i> (Vic), s 11(1)(b), (d)	The Victorian Act does not apply to information that is contained in a document that is 'kept in a library, art gallery or museum for the purposes of reference, study or exhibition' and 'Archives within the meaning of the Copyright Act 1968 of the Commonwealth'
		The New South Wales and Tasmanian Acts do not have similar exceptions. However, the exceptions concerning publicly available documents may be applicable.
Information held by certain institutions	<i>Privacy Act 1988</i> (Cth), s 6(1)	'Record' under the Commonwealth Act does not refer to: 'Commonwealth records as defined by subsection 3(1) of the <i>Archives Act 1983</i> (Cth) that are in the open access period Documents placed in the 'memorial collection' of the Australian War Memorial (memorial collection is defined as 'all historical material that is owned by the Memorial from time to time': <i>Australian War Memorial Act 1980</i> (Cth), s 3)
	<i>Information Act 2002</i> (NT), s 68(1)(d)	The NT IPPs (except for IP 1 and 3) do not apply to information that 'is recorded information of permanent value that forms part of the Territory Archives but is not a record'
	<i>Information Privacy Act 2000</i> (Vic), s 11(1)(c)	The Victorian Act does not apply to 'public records available for public inspection under the <i>Public Records Act 1973</i> '

TABLE 5.3 - Comparative Table of Privacy Principles

Principle	CTH Public Sector	CTH Private Sector	NSW	VIC	NT	TAS
<i>Collection</i>						
Scope restrictions	IPP 1	NPP 1	s 8	IPP 1	IPP 1	IPP 1
Lawful purpose						
Directness	IPP 1	NPP 1	s 8	IPP 1	IPP 1	IPP 1
Notification of purpose						
	IPP2	NPP1 NPP 1	s 9 s 10	IPP1 IPP 1	IPP 1 IPP 1	IPP 1 IPP 1
<i>Storage</i>						
Data Quality	IPP 3	NPP 3	s 11	IPP 3	IPP 3	IPP 3
Security/retention						
	IPP 4	NPP 4	s 12	IPP 4	IPP 4	IPP 4
<i>Access/Amendment</i>						
Openness	IPP 5	NPP 5	s 13	IPP 5	IPP 5	IPP 5
Access	IPP 6	NPP 6	s 14	IPP 6	IPP 6	IPP 6
Amendment	IPP 7	NPP 6	s 15	IPP 6	IPP 6	IPP 6
<i>Use/disclosure limitations</i>						
Use	IPP 10	NPP 2	s 17	IPP 2	IPP 2	IPP 2
Disclosure	IPP 11	NPP 2	s 18	IPP 2	IPP 2	IPP 2
<i>Other</i>						
Unique identifiers		NPP 7		IPP 7	IPP 7	IPP 7
Anonymity		NPP 8		IPP 8	IPP 8	IPP 8
Transborder data flow restrictions		NPP 9		IPP 9	IPP 9	IPP 9
Sensitive information		NPP 10	s 19	IPP 10	IPP 10	IPP 10

TABLE 5.4 - Enforcement Bodies

Commonwealth/Australian Capital Territory	Federal Privacy Commissioner
New South Wales	NSW Privacy Commissioner
Northern Territory	NT Information Commissioner
Tasmania	Tasmanian Ombudsman
Victoria	Victorian Privacy Commissioner

5.1.4 Health Records laws

(i) Coverage

The majority of the information privacy laws outlined above, including both the private sector and public sector requirements in the Commonwealth Act, apply to personal health information as well as other categories of personal information. However, the private sector provisions in the Commonwealth Act do not apply to health information contained in the records of current or former employees or to health information held by small business operators which do not provide health services.

In the case of the Australian Capital Territory, Victoria and New South Wales, health records are governed by separate 'stand alone' health records laws which regulate personal health information collected and used by public sector bodies and private sector organisations located in those jurisdictions. The health records laws are summarised in Table 5.5.

In the case of private sector organisations located in the Australian Capital Territory, Victoria and New South Wales any obligations under health records laws are additional to their obligations to comply with the NPPs in the Commonwealth Act.

(ii) Health information

The expressions 'health information' and 'health service provider' are both broadly defined in each of the Acts. The definitions in s 3(1) of the Victorian *Health Records Act* are reasonably typical.

'Health information' includes information or opinion about an individual's physical, mental or psychological health (at any time), disability (at any time), expressed wishes about the future provision of health services to him or her, personal information concerning or relating to health services provided to him or her, personal information collected in connection with his or her donation, or intended donation, body parts, organs or body substances or identifiable genetic information which could be predictive of his or her health (at any time) or that of his or her descendants.

A 'health service' includes any activity performed in relation to an individual that is intended or claimed to assess, maintain or improve the individual's health; diagnose the individual's illness, injury or disability; treat the individual's illness, injury or disability or suspected illness, injury or disability; a disability service, palliative care service or aged care service;

and the dispensing on prescription of a drug or medicinal preparation by a pharmacist.

TABLE 5.5 - Australian health records laws

Jurisdiction	Legislation	Coverage	Privacy Principles
Australian Capital Territory	<i>Health Records (Privacy and Access) Act 2002 (ACT)</i>	Health records in both the public and private sectors	Privacy principles in Schedule 1.
New South Wales	<i>Health Records and Information Privacy Act 2002 (NSW)</i>	Health records in both the public and private sectors	Health Privacy Principles in Schedule 1
Victoria	<i>Health Records Act 2001 (Vic)</i>	Health records in both the public and private sectors	Health Privacy Principles, Schedule 1

(iii) Exceptions to information that qualifies as health information

The Victorian and New South Wales health records laws both contain a number of exceptions to information that qualifies as health information. These include exceptions for generally available information or the information of individuals who have been dead for more than 30 years.

(iv) The health privacy principles

The health privacy principles in the health records laws are based on those contained in the Information Privacy Acts and cover collection, use, disclosure, quality, security and disposal of information as well as containing rights of access and amendment. There also additional principles which deal with health specific issues such as the closure of medical practices.

(v) Oversight and enforcement of privacy requirements

The ACT and Victorian health records laws are subject to enforcement and oversight by the ACT and Victorian Health Commissioners, respectively. The NSW law is subject to enforcement and oversight by the New South Wales Privacy Commissioner.

5.1.5 Anti-surveillance laws

Information privacy laws are supplemented by laws which prohibit specific surveillance activities including telecommunications interception and use of surveillance devices such as video cameras.

Those which are most likely to be of relevance are the laws which regulate the surreptitious use of surveillance devices, including laws which regulate the use of listening devices, video surveillance and workplace surveillance. The main laws are listed in Table 7.6.

TABLE 5.6 – Key anti-surveillance laws

ACT	<i>Listening Devices Act 1992 (ACT)</i>
CTH	<i>Telecommunications (Interception) Act 1979 (Cth)</i>
NSW	<i>Workplace Video Surveillance Act 1988 (NSW); Listening Devices Act 1984 (NSW)</i>
NT	<i>Surveillance Devices Act 2000 (NT)</i>
QLD	<i>Invasion of Privacy Act 1971 (Qld)</i>
SA	<i>Listening and Surveillance Devices Act 1972 (SA)</i>
TAS	<i>Listening Devices Act 1991 (Tas)</i>
VIC	<i>Surveillance Devices Act 1999 (Vic)</i>
WA	<i>Surveillance Devices Act 1998 (WA)</i>

5.1.6 Common law

Common law is the case law that is based upon the decisions of judges, built up case by case over the centuries. To date, the Australian common law has differed from that in New Zealand and the United States in that it does not have a specific common law action that protects the privacy of information.² However, there are other common law actions that can be used to protect certain aspects of privacy.

The main source of common law privacy protection is via the action for breach of confidence (see section 6.5 below). Personal information may be protected via this action if it has been surreptitiously obtained³ or is subject to an obligation to treat it as confidential.

5.1.7 Privacy Issues Arising at Specific Stages of the e-Research Process

(i) Collection of identifiable personal information via remote instruments (DART DMQ packages)

The collection aspect of the DART e-Research framework involves the use of instruments and other devices for the generation of research data. For example, the objectives of the DART DMQ packages include the provision of online, remote access to pilot working sensors or instruments; and increasing the intelligence of the storage framework by building event triggers.

These activities may involve the collection of information about:

- Researchers and their staff; and
- Third parties (including research subjects and persons whose data is collected incidentally).

Any identifiable information included in data collected from instruments or sensors (and any related metadata that is generated) will need to be treated consistently with any applicable privacy principles.

Research staff should be informed that their personal data is being collected. In the case of research subjects, data should be collected only with their consent or in accordance with ethics clearances as discussed further below.

An aspect of collection requirements which may present difficulty, especially where information is collected as a by-product of research, is the requirement of notification. This is most likely to present problems where the persons whose data is collected are not part of the project. A useful strategy in such cases, if feasible, is to de-identify the data (for example by blurring photo images).

◀ TIP

Data collected from instruments and sensors should be routinely inspected to check for any identifiable personal information which has been inadvertently collected. Where such information is found, the relevant person should be notified or, if possible, the data should be de-identified (for example, via the blurring of an image).

Examples of collection issues raised by demonstrator models

The climatology demonstrator: this involves the collection of information from remote instruments including fixed cameras. These may from to time to time photograph persons who come into range (for example, people on boats). Whether or not that data qualifies as 'personal information' will depend on whether the identity of the persons can 'reasonably' be ascertained. It is possible that a clear image coupled with other contextual information (for example, the name of a boat) may be sufficient to provide for reasonably easy identification. To ensure that such collection is not regarded as unreasonable it would be useful, where feasible, to erect signs warning about the presence of the cameras and details about the collecting institution. To the extent that the information gathered is identifiable, it will be subject to the relevant privacy principles, including notification, security and access.

The crystallography demonstrator: this involves providing researchers with real time video access to the mounted crystal involved in the experiment and the activities of laboratory staff. It is therefore important that laboratory staff are made aware that such filming is taking place. Notice will generally be sufficient to negate any suggestion that the collection is unreasonable and to ensure that it does not contravene specific anti-surveillance laws such as the *Workplace Video Surveillance Act 1988* (NSW). Once again, any identifiable information collected will be subject to the operation of any applicable privacy principles, including those relating to notification, security and access.

(ii) Transfer and storage of data (DART SI packages)

This aspect of the DART project addresses the need to work with data in a secure way with controlled access.

Where the data to be transmitted and stored includes identifiable personal information, two main privacy requirements will arise:

- The requirement to take reasonable steps to protect its security during transfer and storage;

- The requirement to comply with any transborder dataflow restrictions; and
- The requirement to provide for the exercise of any rights of access and amendment.

The data security requirements generally require the taking of reasonable precautions to prevent access or misuse by others. For example IPP 4.1 in the *Information Privacy Act 2000* (Vic) requires that an organisation must take reasonable steps to protect any personal information held from 'misuse and loss and from unauthorised access, modification or disclosure'.

As the DART project involves the electronic transfer and storage of information, this requires attention to a range of measures including:

- Encryption and authentications measures to ensure that information is kept secure both during storage and transmission, that it cannot be tampered with, is kept secret and that the parties to the transmission can be sure that they are who they say they are;
- Network protection mechanisms such as anti-virus software and operating system controls; and
- Adherence to established security policies and procedures as established by the organisation and/or current standards or industry best practice.

A more detailed discussion of security measures is provided in Chapter 6.

←TIPS

A good way of ensuring that security measures qualify as reasonable is to ensure that they comply with current standards or industry best practice.

It is also important that any migration of data from the system occurs only into a safe environment with equivalent protection.

It is also necessary to consider requirements concerning data quality and destruction of data. As described above, according to the storage principles, measures will need to be adopted that ensure data is relevant, up to date and complete for the purposes for which it is used. Information must also be

destroyed or de-identified (for example, blurred) where it is no longer needed.

(iii) The submission of data and results by researchers into repositories (CR packages)

This aspect of DART involves four categories of information that may give rise to privacy issues.

(a) Information obtained from research subjects in relation to their practices and views on research

If the individuals about whom personal information is collected are the subjects of the research study it will be necessary for the researchers to apply for clearance by Human Research Ethics Committees (HRECs). HRECs approve proposed research involving humans based on the National Statement on Ethical Conduct in Research Involving Humans⁴ (National Statement) (including the Form Privacy Statement in relation to identifiable personal data).

Under the National Statement, researchers must ensure that the privacy, confidentiality and cultural sensitivities of research subjects or collectivities is maintained (NS 1.19).⁵ Therefore, HRECs must carefully assess whether research proposals provide the degree of protection that is required for participants.

The Human Research Ethics Handbook,⁶ which provides commentary of the National Statement, requires HRECs to carefully assess the 'processes of collection, storage, access to and use of personal information' and whether these processes will provide the degree of protection that is 'promised to participants.'⁷

The Human Research Ethics Handbook also requires that a HREC must be sufficiently informed on all aspects of a research protocol (as required under NS 2.8), including information protection. Furthermore, a HREC must also be satisfied that research proposals conform to relevant Commonwealth, State or Territory legislation concerning privacy or codes of practice (NS 18).

Research involving Aboriginal and Torres Strait Islander individuals, groups or communities must follow the NHMRC Guidelines on Ethical Matters in Aboriginal and Torres Strait Islander Health Research (Interim 1991).⁸ Furthermore, research funded by the Australian Institute of Aboriginal and Torres Strait Islander Studies (AIATSIS) must comply with AIATSIS guidelines (NS 9).

In light of these requirements, particular care is required by researchers in drafting the consent forms that will be signed by research subjects to ensure that subsequent uses and disclosures are consistent with use and disclosure limitation principles. To avoid rejection, researchers must also outline in detail how they will provide the required protection measures in ethics application and privacy forms which they submit to HRECs.

(b) Information obtained from researchers in relation to establishing ways to improve their information management practices

Where DART researchers are placed within research groups to provide assistance in establishing information management practices, they may have to collect or use data that contains personal information about researchers in these groups. If this is the case, the appropriate privacy principles will need to be followed to ensure that this information is kept private.

Furthermore, the information management practices which need to be established with the assistance of DART researchers should comply with privacy obligations. For example, research groups should ensure that they obtain appropriate consent from research subjects before they start collecting, using and disclosing data.

(c) Historical data and other data from personal repositories

Researchers conducting research that produces data which will be placed within the DART repositories are responsible for complying with any relevant privacy principles. However it will also be necessary for the DART team to ensure that there has been consent by individuals for all intended uses and disclosures when their identifiable personal data is migrated into DART repositories.

In many cases involving historical data (including information concerning indigenous peoples), it may not be possible to receive approval from those that provided the information. Inability to obtain consent may be due to several reasons, including the fact that the participant can no longer be located or contacted, or even due to the death of the participant.

Under NS 1.7 of the National Statement, the consent of individuals or collectivities must be obtained before research is conducted, except in specific circumstances, such as (NS 1.11):

- De-identified data in epidemiological research (see NS 14.4);
- Research involving persons that are highly dependant upon medical care (see NS 6.9);

- Use of human tissue samples (see NS 15.8);
- Human genetic research (16.13);
- Observational research conducted in public places and anonymous surveys (see NS 17.2); and
- Research in relation to linkages of records (see NS 18.5).

For example, under NS 14.4, an HREC can approve access to 'identifiable or potentially identifiable data' in regards to epidemiological research without the consent of those that the data identifies if it is satisfied that:

- the procedures needed to obtain consent are likely to cause unnecessary anxiety to those whose consent is sought or would prejudice the scientific value of the research and there would be no disadvantage suffered by participants or their relatives or any collectivity; or
it is impossible practically due to the age, quantity or accessibility of the relevant records to obtain consent;
and
- the public interest in the research outweighs to a substantial degree the public interest in privacy.

← TIP

Consent plays a critical role in minimising privacy problems. It is important to ensure that the scope of the consent given by research subjects is sufficiently broad to cover any anticipated uses and disclosures within DART. Accordingly, attention needs to be given to the drafting of consent statements having regard to all intended uses or purposes.

Example of consent issue raised by a demonstrator model

The Women on Farms demonstrator: this demonstrator involves the display and sharing of information submitted by women farmers about their life in rural Australia on a website. The display of information is organised according to the Women on Farms gatherings that have been conducted each year since 1990. As the information includes photographs, quotations and descriptions of individuals, consent may be needed before personal information such as this is displayed on the website. However, the website contains historical information and it may not be possible to obtain the consent of every individual. In these instances, consent may not be needed under NS 14.4 as outlined above. On the other hand, information may be de-identified where possible.

(d) Digital objects that are subject to Creative Commons and Science Commons licences

Additional privacy considerations will need to be addressed with digital objects that are accompanied by Creative Commons (CC) or Science Commons (SC) licences. As described in Chapter 6, CC and SC licences allow owners of information to license their copyright, as licensors, to the public whilst still retaining their copyright ownership.

Where the digital object contains personal information about the licensor, the attachment of a CC or SC licence may indicate that the licensor consents to others using any identifiable personal information about them.

On the other hand, where the digital object contains identifiable personal information about a third party who is not the licensor, the licensor and licensees will have to ensure that CC or SC licence terms concerning the disclosure of the information is not inconsistent with any legal requirements under privacy laws. In these circumstances, a licensor may have to obtain the consent of the third party, de-identify the information or draft a licence that restricts the collection, use and disclosure of the information.

(iv) Annotation and assessment of research data (AA work packages)

The AA work packages aim to provide mechanisms that allow users to annotate items within DART repositories and enhance collaborative work practices in research teams.

Personal information may be contained in annotations (or contributions) to:

- Research data, reports and publications within the DART repositories;
- Collaborative works where real time annotations are made of digital objects such as images, videos and 3-D objects; and
- Hosted wikis that are linked to research data repositories.

As is the case with all identifiable personal information, any such information found within annotations or contributions made to any digital objects (or any associated metadata) will have to be protected under the relevant privacy laws.

Persons who make and store annotations or contributions should ensure that these additions comply with privacy requirements, such as collection, use, and notification, where they contain personal information. DART may therefore have to monitor the content of annotations and contributions.

Examples of annotation issues raised by demonstrator models

Crystallography demonstrator: the DART project will allow researchers to annotate 3-D protein structures that have been developed using crystallography techniques. These annotations may contain personal information such as the names of researchers or their work place. These annotations should comply with the relevant privacy requirements in regards to collection, use and notification.

Climatology demonstrator: climatology data may be annotated with information such as the person who collected the data and who has analysed the data. This information may be considered personal information and be subject to privacy laws.

The Women on Farms demonstrator: persons who submit information to the Women on Farms website may annotate photographs with information about other individuals within the picture, such as their names and where they live. This information will be subject to privacy requirements. Thus, the consent of these individuals will be required before the information should be used or disclosed. The person submitting the information is presumed to consent to the use and disclosure of the information.

(v) Discovery and Access (DA work packages)

This final aspect of the DART project aims to improve repository deposit rates, sharing and re-use through permitting end-user control over access and enhancing discoverability.

If depositors of digital objects are to have control over access, DART will have to provide the appropriate security mechanisms that allow depositors to protect any relevant identifiable personal information. The personal information contained within these digital objects and any related metadata may relate to the depositor or a third party. Therefore, the protection required for the information will largely depend upon the consent of the information subject in regards to the purpose and disclosure of the information. The security measures that can be used will be discussed in Chapter 6.

← TIP

If digital objects within DART repositories will be made available through other discovery services, such as the national research discovery service hosted by the National Library of Australia, DART should ensure that these services also provide adequate privacy protection for information.

A further issue concerning access and discovery relates to the provision of statutory obligations concerning access and amendment to information subjects.

Information subjects (including research subjects, researchers, others employed in the research process and third parties) will have a statutory right of access to any identifiable personal information held on the DART database. It is therefore important to implement appropriate measures and procedures for the exercise of these rights and to ensure that these are outlined in the required openness statement as discussed above in relation to access and amendment.

In designing these procedures it is important to bear in mind that the rights of access provided in each Act are subject to a number of exceptions. These may arise, for example, where the information is intermixed with personal information relating to other individuals or with sensitive business information. A useful procedure which can be used when such information is intermixed is to provide access to copies of the applicant's records from which the exempt material has been redacted (for example, in the case of text-based information by masking the exempt material and making a photocopy of the document).

The information privacy laws also contain principles which allow individuals to seek amendment of any data which is incorrect, out of date, misleading or irrelevant to the purpose for which the data was collected. Whether or not specific information is out of date or misleading must be assessed from the context in which it is currently used. This means that historical data will qualify as out of date unless it is used in a way which assumes that it is also currently accurate.

As discussed above, the related retention limitation principles require that data must be de-identified or destroyed if it is no longer needed for any relevant purpose where it may be used or disclosed.

Examples of access issues raised by demonstrator models

Crystallography demonstrator: crystallography researchers may wish to restrict access to personal information contained in images or annotations created as part of the crystallography experiment. For example, access may be restricted to persons directly involved in the experiment, such as members of the laboratory. The relevant personal information could be de-identified, or the consent of the relevant individuals could be obtained, if researchers later wish to disclose experimental data to the public.

The Women on Farms demonstrator: while the aim of the Women on Farms website is to display information about women on farms in Australia, some individuals may not wish to disclose certain information about themselves (for example a woman in a picture may not want her name or face to be displayed). In these cases, the website can withhold the individual's name and/or blur out her face in the photograph.

Women may also wish to amend information that has been placed on the website about themselves that is incorrect, out of date, misleading or irrelevant. In some cases, women disagree in regards to the accuracy of stories that are displayed on the website. The project is currently looking for ways to deal with these issues.

5.1.8 Some more complex privacy issues raised by the DART project

(i) Transborder data flow restrictions

It is a fundamental aspect of DART that information (including raw datasets) will be available for sharing irrespective of jurisdictional boundaries. However, as is clear from Table 5.1, several states still lack privacy laws. In addition, most private sector organisations are excluded from the operation of the private sector provisions in the Privacy Acts via the small business operator exemption. Likewise many overseas countries, including the US, lack comprehensive privacy laws.

This creates difficulty as the majority of Australian privacy laws contain restrictions on the transfer of data to places which lack equivalent protection. Therefore, to the extent that data stored within DART is potentially subject to access and downloading in places which lack equivalent privacy protection, it may be necessary to incorporate contractual privacy obligations into the mechanisms used for access and downloading. (Contracts facilitate compliance with transborder dataflow restrictions by ensuring that personal data receives adequate protection in jurisdictions with less protective privacy regimes).

To the extent that researchers are involved in collaborative research with researchers from countries with stronger privacy laws (for example,

researchers in EU member countries) they may themselves be subject to contractual obligations. If it is desired to include this data within DART then it is important that there are mechanisms available to ensure that these higher standards are imposed.

(ii) Deidentification

It is unlikely that much of the personal data collected and stored as part of DART will be identified by name. However, it is possible that information that was once regarded as de-identified may no longer qualify as such, particularly if combined with other information. For example, it may be possible to identify some individuals from three seemingly innocuous items of information (for example date of birth, postcode and occupation).

The issue of identifiability also arises in the context of visual images. Persons may be potentially identifiable if images are of sufficient quality or coupled with other contextual data. For example, in the Victorian Civil and Administrative Tribunal case of *Ng v Department of Education*,⁹ it was held that it is now 'common ground' that a digital recording (such as a video recording of a teacher holding a class in a school computer room) is personal information. It seems to have been the case in this instance that the teacher's identity was apparent. The position will be different where the images are blurred and there is insufficient contextual information to identify any person filmed.

As outlined above, 'personal information' is information about a person whose identity is apparent, or can 'reasonably be ascertained' from the information. The word 'ascertained' must allow for some resort to extraneous material. Even allowing for the use of external information, the legislation requires an element of 'reasonableness' about whether a person's identity can be ascertained from the information and this will depend upon all the circumstances in each particular case.

←TIP

When determining whether or not data has been sufficiently de-identified it is important

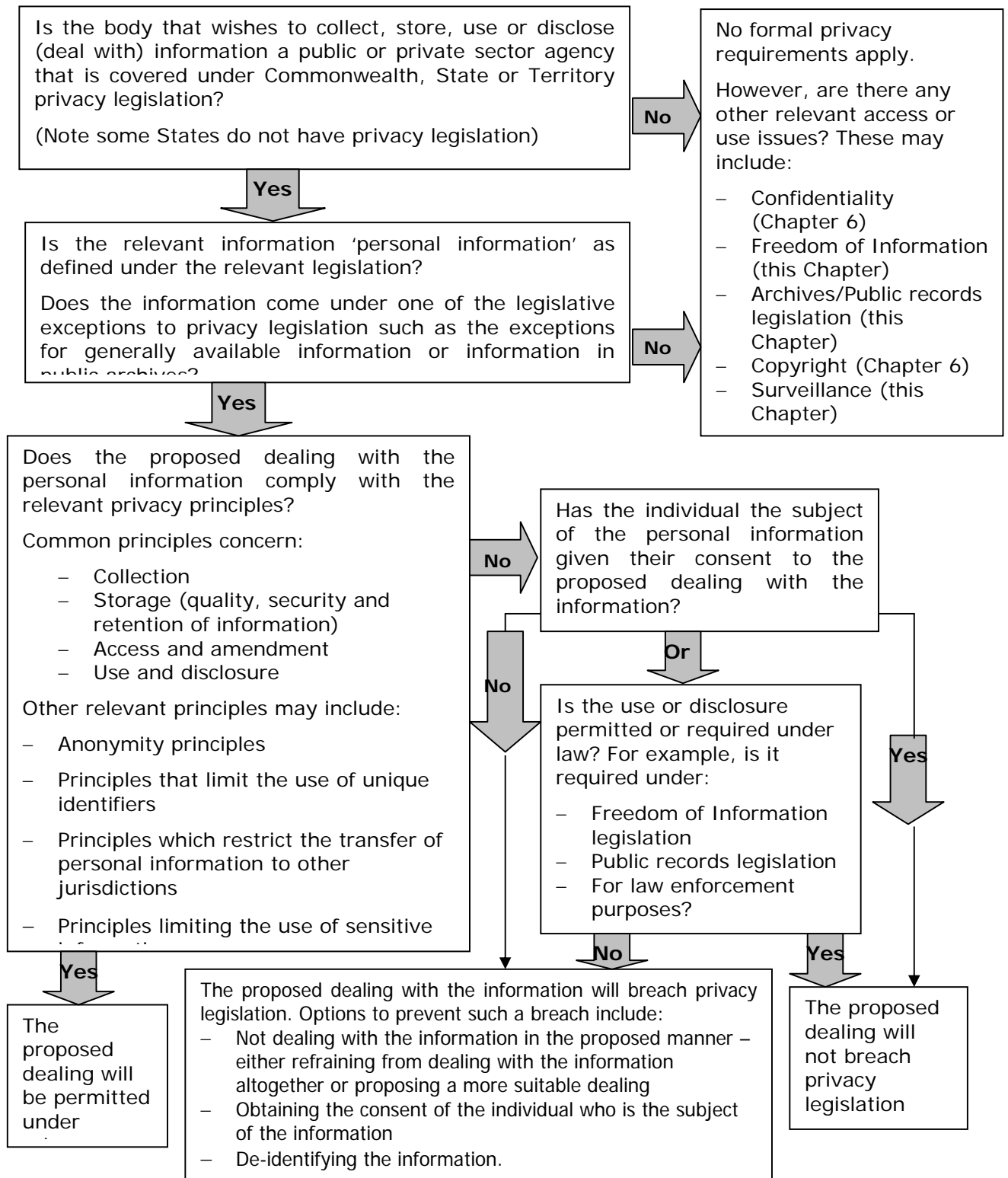
not just to consider the specific data alone but also whether it might reasonably be combined with other extraneous material to disclose the identities of any individuals to which it relates.

Examples of de-identification issues raised by demonstrator models

The crystallography demonstrator: as described above, this demonstrator involves providing researchers with real time video access to the mounted crystal and the activities of laboratory staff. The recording of research staff will be considered personal information where the researcher's identity can be 'reasonably' ascertained from the videos and/or any extraneous material, such as records of who works at the relevant laboratory that may be available on the Internet. Where possible (which may be difficult in the case of real time feeds), the relevant segments of footage may need to be blurred to disguise the identity of the individual (de-identification).

The Women on Farms demonstrator: the identity of women whose images are placed on the Women on Farms website may be ascertainable where the images are very detailed or are accompanied by other contextual information, such as details of where the individual lives. De-identification will be essential where the individual does not consent to the disclosure of this information.

Figure 5.1 - Information Privacy



5.2 FREEDOM OF INFORMATION

The Commonwealth, and all of the Australian States and Territories, have enacted Freedom of Information (FOI) Acts as set out in Table 5.7. These apply to public sector bodies in the relevant jurisdiction. For example, Victorian public sector bodies such as Monash University are governed by the *Freedom of Information Act 1982* (Vic).

Subject to a number of exceptions and exemptions, FOI legislation provides members of the public with the legally enforceable rights of access to documents (including electronic records) held by public sector agencies. It also entitles them to request an agency to amend their personal records if they are incorrect, out of date or misleading.

Each FOI Act specifies the procedures to be followed by applicants in making requests for access and by agencies in processing such requests. Requests for access must be made in writing and specify the particular documents to which access is sought. Agencies are required to provide assistance to applicants in framing their requests for access and are also required to deal with requests expeditiously within specified time limits and to provide reasons for any adverse decisions.

Applicants may request to be provided with access in a number of forms, for example, through inspection of the document; being provided with a copy of the document; being given the opportunity to hear or view sounds or visual images; or being provided with a written transcript. They are usually required to pay applications fees and charges based on the time spent in searching for documents and deciding upon requests.

The access rights in the FOI legislation are confined to documents in the possession of Ministers and government agencies, such as government departments, statutory authorities, local councils and other bodies created for public purposes. Except where they are created as privately funded and operated institutions, universities and other tertiary education institutions are subject to the operation of FOI laws. A document is regarded as being in the possession of a body if it is subject to its control. Therefore, whether documents held by the DART project are subject to FOI laws will depend upon whether they are subject to the control of a public university such as Monash or of some other public body.

Table 5.7 - Australian Freedom of Information legislation

Jurisdiction	Act	Access provisions	Exemptions	Amendment provisions
Australian Capital Territory	<i>Freedom of Information Act 1982 (Cth)</i>	Part 3	Part 4	Part 5
Commonwealth	<i>Freedom of Information Act 1989 (ACT)</i>	Part III	Part IV	Part V
New South Wales	<i>Freedom of Information Act 1989 (NSW)</i>	Part 3	Schedule 1	Part 4
Northern Territory	<i>Information Act 1992 (NT)</i>	Part 3	Part 4	Part 3
Queensland	<i>Freedom of Information Act 1992 (Qld)</i>	Part 3, Division 1	Part 3, Division 2	Part 4
South Australia	<i>Freedom of Information Act 1991 (SA)</i>	Part 3	Schedule 1	Part 4
Tasmania	<i>Freedom of Information Act 1991 (Tas)</i>	Part 2	Part 3	Part 4
Victoria	<i>Freedom of Information Act 1982 (Vic)</i>	Part III	Part IV	Part V
Western Australia	<i>Freedom of Information Act 1992 (WA)</i>	Part 2	Schedule 1	Part 3

The term 'document' is broadly defined to include not just traditional paper documents but also electronic records (including information forming parts of

databases), photographs, films and sound recordings. In addition, there may be a requirement to generate a new document from information held in a database.

The rights of access in FOI laws are subject to exceptions in respect of specific categories of documents as summarised in Table 5.8. These include exceptions for documents which are otherwise publicly accessible (for example, via public records laws or library collections) and, in the case of the some of the Acts, exceptions for some older 'prior documents' which were created prior to the enactment of the relevant FOI law.

The FOI Acts are subject to a number of exemptions which are designed to protect governmental, agency and third party interests. Those which are most likely to be relevant to documents forming part of the DART project are summarised in Table 5.9. They include exemptions for personal information relating to persons other than the applicant, trade secrets and other sensitive business information and information subject to obligations of confidentiality. Other exemptions which are likely to be of relevance include exemptions for research data and for other data which cause harm to an agency if disclosed.

Where information within a document is exempt, it may be necessary to consider whether or not the exempt matter can be redacted so as to allow provision of access to the remainder of the document.

← TIP

Information which will cause potential harm to a tertiary institution (for example by exposing the institution to commercial disadvantage) is potentially subject to exemption. It may be useful to develop some means of identifying information which may qualify for exemption. However, it should also be noted that simply categorising information as being 'Confidential' or 'Commercial in confidence' will not necessarily qualify it for exemption; the test to be applied is that contained in the relevant exemption/s.

Where a document contains third party information such as identifiable personal information or financial or business information about an identifiable individual or organisation there is generally a requirement, where practicable, to consult with that person or organisation before making any decision to provide access to the document. Persons who have a right to be consulted

concerning disclosure will usually have the right to appeal against any decision to grant access to a document contrary to their wishes.

•TIP

The third party exemptions in FOI laws will be potentially applicable where information stored within the DART project can be traced to some identifiable person or body. To the extent that data which is covered by FOI legislation contains such information, it may be useful to develop some means of readily identifying that it does so and, where practicable, to link to it any available information concerning how to contact the persons or bodies to which it relates

Individuals can apply in writing for their personal records to be amended or annotated where the information is incomplete, incorrect, out of date or misleading. Those procedures enhance the information privacy rights of individuals who have previously obtained access to their personal information. The extent to which statements of fact may be regarded as incorrect, and therefore requiring amendment, depends on the context in which they are recorded. Likewise, the mere fact that information is old is not sufficient for it to be considered out of date; whether it is out of date depends on the context in which it is used. It therefore follows that a document containing an accurate record of events which occurred or assessments which were made at the time it was created will not generally require amendment.

Where a request for the amendment of personal records is unsuccessful, an agency is required if requested by the applicant to do so, to add to the record an annotation which sets out with the applicant's reasons for the amendment request and the amendments they wish to make. An agency may also, if it so wishes, add its own comments to any such annotation (for example as provided under s 51E of the Commonwealth FOI Act).

Table 5.8 - Key categories of documents excluded from access requirements

Exception	Jurisdictions	Sections in the FOI Acts
<p>Prior documents – documents created before a specified date, usually 5 years before the commencement of the relevant access provisions). NB this category is generally subject to an exception in respect of an applicant’s own personal information.</p>	Commonwealth	s 12 (2)
	Australian Capital Territory	s 11(2)
	Northern Territory	s 13
	Victoria	s 67(2)
	Western Australia	s 8(2)
<p>Documents otherwise available. These documents may include: library reference materials; documents which have been placed in collections by private persons; and documents available via other means.</p>	Commonwealth	s12(1)
	Australian Capital Territory	s 11(1)
	New South Wales	s 25(1), sch 1 cl 19
	Northern Territory	s 12(2) and (3)
	Queensland	ss 22, 23
	South Australia	s 20(1), sch 1 cl19
	Tasmania	ss 9, 10
	Victoria	s 5(1) ('documents'), 14(1)(a)
Western Australia	ss 6, 7	

Table 5.9 - Exemption provisions which are likely to be relevant to research data

Exemption	Application	FOI legislation
Documents affecting personal privacy or personal affairs. (Such information is exempt only if its disclosure would be 'unreasonable' or contrary to the public interest.)	Commonwealth	s 41
	Australian Capital Territory	s 41
	New South Wales	Schedule 1, cl 6
	Northern Territory	s 56a
	Queensland	s 44
	South Australia	Schedule 1, cl 6
	Tasmania	s 26
	Victoria	s 33
	Western Australia	Schedule 1, cl 3
Documents containing confidential information. (These provisions vary considerably. Some FOI Acts offer protection where disclosure would provide the basis for an action for breach of confidence, others protect confidential information more generally and some offer protection only where the disclosure will harm an agency's ability to acquire such information in the future.)	Commonwealth	s 45
	Australian Capital Territory	s 45
	New South Wales	Schedule 1, clause 13
	Northern Territory	s 55
	Queensland	s 46
	South Australia	Schedule 1, cl 13
	Tasmania	s 33
	Victoria	s 35
	Western Australia	Schedule 1, cl 8
Documents containing information relating to research. (Once again these exemptions vary considerably in their scope. Some are confined to the results of scientific or technical research undertaken by an officer of an agency and others extend to all research, irrespective of whether it has commenced or been completed. The Cth Act is confined to research carried out by the ANU and CSIRO.)	Commonwealth	s 43a
	Australian Capital Territory	Nil
	New South Wales	Schedule 1, cl 8
	Northern Territory	s 57
	Queensland	S 45(3)
	South Australia	Schedule 1, cl 8
	Tasmania	s 32(b)
	Victoria	S 35
	Western Australia	Schedule 1, cl 10
Documents which if disclosed may cause harm to an agency's operations, financial or property interests or its business affairs. (Once again these provisions vary considerably in their scope and wording).	Commonwealth	ss 39, 40, 43
	Australian Capital Territory	ss 9, 40, 43
	New South Wales	Schedule 1, cls 7, 15
	Northern Territory	ss 57(3), 58
	Queensland	ss 45, 49
	South Australia	Sch 1, cls 7, 15
	Tasmania	s 32

	Victoria	s 34(4)
	Western Australia	Schedule 1, cl 10(6)

A person who receives an adverse decision in relation to a request for access or amendment or who wishes to dispute charges levied for access must usually first seek internal review within an agency. If they are not eligible to apply for internal review or are dissatisfied with the outcome of any internal review, they are entitled to apply for external review to the review bodies set out in Table 5.10.

Table 5.10 - External Review Bodies (FOI)

Jurisdiction	External Review Body
Commonwealth	Commonwealth Administrative Appeals Tribunal (also Commonwealth Ombudsman)
Australian Capital Territory	Australian Capital Territory Administrative Appeals Tribunal (also ACT Ombudsman)
New South Wales	Administrative Decisions Tribunal
Northern Territory	Northern Territory Information Commissioner
Queensland	Queensland Information Commissioner
South Australia	South Australian Ombudsman and South Australian District Court
Tasmania	Tasmanian Ombudsman
Victoria	Victorian Civil and Administrative Tribunal (also Victorian Ombudsman)
Western Australia	West Australian Information Commissioner

Examples of access issues raised by demonstrator models

Crystallography demonstrator: Crystallography documents, such as CCD and protein structure images, may be subject to requests for access under FOI legislation (for example, by persons from other research institutions) to the extent they are in the possession of a public body. However they may qualify for exemption, for example on the basis that they contain research information and are also likely to cause harm to the relevant institution if disclosed.

Climatology demonstrator: Members of the public, such as fishermen, may wish to access documents containing climate readings and maps under FOI legislation. Whether that are able to do so will depend on whether the documents can be regarded as being in possession of a public body covered by the relevant FOI Act and and, if so, whether they qualify for exemption.

Digital History demonstrator: the Nelson Project aims to make the N.F. Nelson report and associated photographic collections available to communities in Cape York by digitising the original report. Although it will be restricted to the relevant communities in Cape York, other members of the public may request access to the digital forms of the manuscript, plans and photographs via FOI legislation, to the extent that the qualify as being in the possession of a public body. However, it is likely that these documents will qualify for exemption on personal privacy grounds and under any exemptions which specifically protect sacred and cultural information. To the extent the information was originally provided in circumstances imparting an obligation of confidence, it may also qualify for exemption under confidentiality exemptions.

5.2.1 Some more complex FOI issues raised by the DART project

(i) Possession

It is unclear to what extent information held by DART will be regarded as being in the possession of different persons and organisations which potentially have access to it.

Generally speaking what is required is legal or constructive possession (ie, the right and power to deal with the document).¹⁰ Arguably, an agency with a right of access to a jointly owned database has a constructive right of access to the data contained in it.¹¹

(ii) The effectiveness of confidentiality requirements

It is likely that contractual provisions will seek to limit the granting of access to third parties. While the existence of any such obligations will make it more likely that the data to which they relate will fall within exemptions which protect confidential information and agency operations, they will not necessarily preclude access under all of the FOI Acts.

(iii) Jurisdictional issues

It is possible that the same data set will qualify as being in the possession of researchers and others in multiple jurisdictions, including overseas countries with FOI laws. This may have the consequence that data which would be protected via exceptions and exemptions in the FOI legislation which applies in the jurisdiction in which it was created will receive a lesser level of protection within DART (because it is potentially accessible via other Acts which offer lesser levels of protection).

5.3 ARCHIVES/PUBLIC RECORDS LEGISLATION

Archives/public records legislation is concerned with the management of public records and the preservation of older documents so that they can be accessed for historical purposes. The laws which are summarised in Table 5.11 generally contain provision for regulation or guidance concerning agency record management and records disposal practices. They also contain provision for the transfer of records of historical significance to the relevant archival authority and procedures for access to that information once it is in the open access period.

Data collected and generated within DART will be subject to archives/public records laws to the extent that it qualifies as a public record. The definition in the Commonwealth *Archives Act* is reasonably typical. 'Commonwealth record' is defined as: 'a record that is the property of the Commonwealth or of a Commonwealth institution'; or a record that is declared a Commonwealth record under a regulation (s 3(1)).¹² The term 'record' includes a document (written or printed) or object (such as a sound recording, coded storage device, magnetic tape or disc, photograph, map, film, microform, plan, model, painting or other graphic or pictorial work) that has been kept because of any information or matter it contains or its connection with any person, event, circumstance or thing (s 3(1)).

Records in the possession of publicly funded universities and other public institutions (including research data) are subject to archives/public records requirements. For example, those in the possession of Monash University should be handled and disposed of in prescribed ways for archival purposes as specified in s 12 of the Victorian *Public Records Act 1973*. The prescribed procedures which must be followed include those set out in the Higher and

Further Education Institution Retention and Disposal Authority (PROS 02/01) which covers research records.¹³ In addition, any records that have been classified as 'permanent' (ie, worthy of permanent retention) under a relevant disposal schedule must comply with Victorian Electronic Records Strategy (VERS), Standard for Electronic Recordkeeping (PROS 99/007).¹⁴

The storage and retention of data will also be affected by any requirements imposed by funding agencies and by the Joint NHMRC/ AV-CC Statement and Guidelines on Research Practice.¹⁵ For example, para 2.3 of the latter provides that:

Data must be held for sufficient time to allow reference. For data that is published this may be for as long as interest and discussion persists following publication. It is recommended that the minimum period for retention is at least 5 years from the date of publication but for specific types of research, such as clinical research, 15 years may be more appropriate.

There is also a requirement that data management should comply with relevant privacy protocols, such as the Australian Standard on personal privacy protection in health care information systems (Australian Standard AS 4400-1995).¹⁶

Table 5.11 – Open access periods under Archives/Public Records laws

Jurisdiction	Open Access period
Commonwealth	30 years
Australian Capital Territory	20 years
New South Wales	30 years
Northern Territory	30 years
Queensland	30 years
South Australia	15 years
Tasmania	25 years
Victoria	25 years
Western Australia	25 years

Example of public records issues raised by a demonstrator model

The Women on Farms demonstrator: This demonstrator involves the display and sharing of information submitted by women farmers about their

life in rural Australia on a website. Provided that the material on the website is simply a copy of documents retained in hard copy, any curation requirements will be confined to the originals. However, to the extent that the digital version contains original annotations of historical significance (for example additional information provided by research subjects) then it will be necessary to consider whether these are worthy of longer term retention.

5.3.1 Some more complex public records issues raised by the DART project

Data retention/disposal

Under current procedures, much primary research data is disposed of in accordance with any applicable disposal schedules (frequently after 5 years). It will need to be decided whether data uploaded into DART is intended to be kept for longer than this and also to ensure that any disposals are not inconsistent with any applicable public record-keeping requirements.

In the case of identifiable personal data there are usually requirements arising under information privacy legislation and ethics clearances for data to be destroyed or deidentified after a specified period. It will be important to have some means for tagging the data in order to ensure that these requirements are met.

ENDNOTES

¹ W L Morison, *Report on the Law of Privacy to the Standing Committee of Commonwealth and State Attorneys-General*, Report No 170/1973 (1974), [1].

² However, in the light of recent developments in the UK and New Zealand, and comments made by members of the Full Court of the High Court in *Australian Broadcasting Corporation v Lenah Game Meat Pty Ltd* (2002) 208 CLR 19 it is possible that such a tort may develop in the future.

³ *Lord Ashburton v Pape* [1913] 2 Ch. 469.

⁴ This can be accessed at: National Health and Medical Research Council, *National Statement on Ethical Conduct in Research Involving Humans* (2005) <<http://www.nhmrc.gov.au/publications/synopses/e35syn.htm>>.

⁵ A 'collectivity' is a 'distinct human group' that has its own social structure that links members with a common identity and customs. It also has a leader or other persons that represent the collective interests of the group when dealing with researchers. An example of a collectivity is an indigenous community: National Health and Medical Research Council, *National Statement on Ethical Conduct in Research Involving Humans* (2005) 31 <<http://www.nhmrc.gov.au/publications/files/e35.pdf>>.

⁶ This can be accessed at: National Health and Medical Research Council, *Human Research Ethics Handbook* (2005) <<http://www.nhmrc.gov.au/publications/synopses/e42syn.htm>>.

⁷ National Health and Medical Research Council, *Human Research Ethics Handbook* (2001) C14 <<http://www.nhmrc.gov.au/publications/hrecbook/pdf/hrechand.pdf>>.

⁸ This can be accessed at: National Health and Medical Research Council, *Guidelines on Ethical Matters in Aboriginal and Torres Strait Islander Health Research* (1991) <<http://www.nhmrc.gov.au/publications/files/e11.pdf>>.

⁹ *Ng v Department of Education* [2005] VCAT 1054.

¹⁰ See generally: *Re Guide Dog Owners and Friends Association and Commissioner for Corporate Affairs* (1988) 2 VAR 405.

¹¹ *Re Shubert and Department of Premier and Cabinet* (2001) 19 VAR 35.

¹² Archives *Regulations 1984* (Cth) regulations 2A and 2B. The term also includes records of Royal Commissions (s 22).

¹³ This authority can be accessed via the website of the Victorian Public Records Office at: Public Record Office Victoria, *Public Record Office Victoria* (2006) <<http://www.prov.vic.gov.au>>.

¹⁴ This can be accessed via the website of the Victorian Public Records Office at: Public Record Office Victoria, *Public Record Office Victoria* (2006) <<http://www.prov.vic.gov.au>>.

¹⁵ National Health and Medical Research Council, *Joint NHMRC / AVCC Statement and Guidelines on Research Practice (1997)* (2005) <<http://www.nhmrc.gov.au/funding/policy/researchprac.htm>>.

¹⁶ [2.1].

6 INFORMATION SECURITY

6.1 INTRODUCTION

Information security relates to the safeguarding or protecting of information or data, regardless of the form in which the information or data appears. The U.S. National Information Systems Security Glossary defines *information systems security (INFOSEC)* as the:

'Protection of information systems against ... unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users' or the provision of service to authorized users, 'including those measures necessary to detect, document, and counter such threats.'¹

Information security is vital to the DART project because of the inherent risks associated with information in the on-line environment and because of the need to control access to information resources. It is essential to manage security risks in order to build *trust* in the DART e-Research infrastructure.

Why is information security essential?

It is essential to ensure that:

- only those who are authorised have access to information systems
- those who are not authorised do not have access to information systems
- the integrity of information is protected against unauthorised amendments, additions, deletions or interceptions
- information systems are available to those who are authorised to have access

In the absence of adequate information security users will not have sufficient *trust* in a collaborative e-Research infrastructure.

This chapter surveys the relevant information security issues and principles in relation to the DART project.

6.2 OBJECTIVES OF INFORMATION SECURITY

The three traditional objectives of information security, sometimes known as the *CIA triad*, are:

- Confidentiality;
- Integrity; and
- Availability.

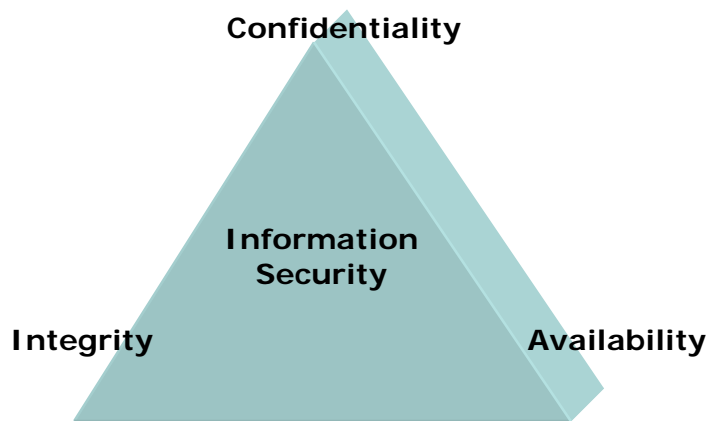


Figure 6.1 - The CIA triad

Additional objectives that are commonly added to the CIA triad are:

- Accountability;
- Non-repudiation;
- Authentication; and
- Privacy.

Each of these objectives requires further explanation.

Confidentiality means ensuring that information is available only to authorised users, and is not disclosed or otherwise revealed to unauthorised persons. A duty to keep information confidential can arise in particular circumstances (as discussed in Chapter 5).

Integrity means ensuring that information is consistent and reliable, and has not been subject to unauthorised creation, alteration or destruction.

Availability means ensuring that authorised users have timely and reliable access to data resources, including information, computing resources and communications resources.

Accountability means ensuring that authorised individuals and processes are able to be traced and appropriately held accountable.

Non-repudiation means protecting against a party to a transaction or communication falsely denying that the transaction or communication has occurred. This involves ensuring that the sender has proof of delivery and that the recipient has proof of the identity of the sender.

Authentication means ensuring that the identity of a person or entity one is dealing with is able to be accurately verified.

Privacy, in this context, means the ability of users to control the use of personal information which may be collected or disclosed in a transaction or communication. Information privacy is discussed further in Chapter 5.

It is important that these objectives be pursued in relation to information when it is stored in a medium, such as a data repository, as well as when it is in transit over a network.

6.3 TECHNIQUES FOR SAFEGUARDING INFORMATION SECURITY

No information system can be absolutely secure. This means that information security is best understood as a process of risk management.²

Managing the risks associated with information security depends upon an appropriate combination of:

- Technological measures, including industry standards;
- Policies and procedures; and
- Laws.

It is possible to identify five kinds of techniques, known as *security services*, for safeguarding information security:³

- *Authentication services* which provide assurances of the identity of parties to a transaction or communication, for example, by means of a password or PIN number;
- *Access control services* which protect against unauthorised access to, or unauthorised use, disclosure, alteration or destruction of information resources;
- *Confidentiality services* which protect against information being disclosed or otherwise revealed to unauthorised persons;
- *Data integrity services* which protect against alteration of data in ways contrary to a security policy; and
- *Non-repudiation services* which protect against a party falsely denying that a transaction or communication has occurred.

6.3.1 Information security fundamentals

This section of the chapter explains the fundamental building blocks for information security systems.

(i) Encryption

The principal technological measures for safeguarding information security involve *encryption*. Encryption is the preferred means for ensuring confidentiality, authentication, data integrity and nonrepudiation.⁴

Encryption means the transformation of intelligible data, known as *plaintext*, into unintelligible data, known as *ciphertext*. Similarly, *decryption* is the transformation of *ciphertext* into *plaintext*. Encryption and decryption work by means of a mathematical operation, known as a *cryptographic algorithm*. As it is relatively easy to discover an algorithm, information security systems depend upon the use of a key.

A *key* is an apparently random series of bits that is used by a cryptographic algorithm. The strength of a cryptographic system depends upon the key length.

There are two types of cryptosystem: *symmetric (or private key) cryptography* and *asymmetric (or public key) cryptography*.

(ii) Symmetric (private key) cryptography

Symmetric cryptography, as the name suggests, involves the use of the same key in both encryption and decryption. Although symmetric cryptosystems, such as the Data Encryption Standard (DES), continue to be used, they suffer from well-known difficulties. The difficulties arise because both the sender and receiver must know the same key. This means that the key needs to be exchanged over a communications channel, leading to the possibility of the key being compromised. It also means that there is a need for a different private key for each new party with whom one communicates.

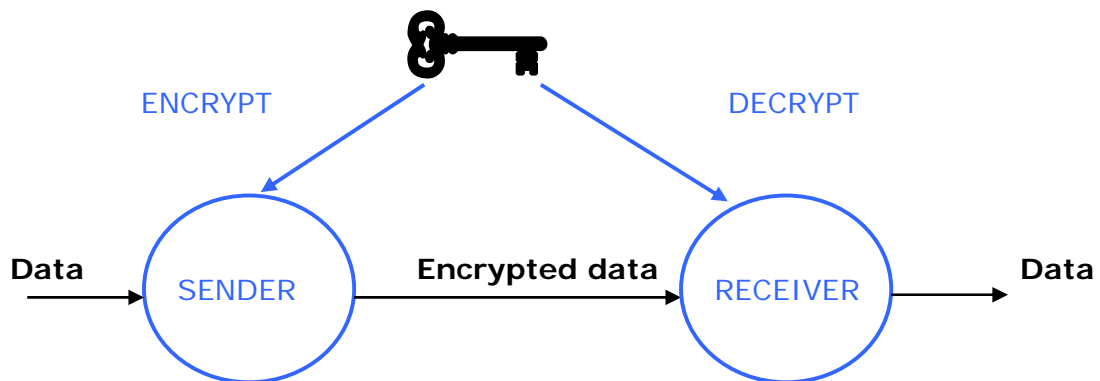


Figure 6.2 - The symmetric cryptography system

(iii) Asymmetric (public key) cryptography

Public key cryptography solves the key exchange problem by using two mathematically related keys:

- A *private key*, which is kept secret; and
- A *public key*, which can be publicly disclosed.

The two keys are known as a key pair. Public key cryptography can operate in one of two modes: *encryption mode* or *authentication mode*.

In *encryption mode*, the public key is used to encrypt information that is sent to the owner of the key pair. As the message can only be decrypted by the private key, which is known only by the owner of the key pair, encryption mode ensures the *confidentiality* of a message.

In *authentication mode*, the private key is used by the owner of the key pair to encrypt a message. As the message can only be decrypted by the public key that is associated with the private key, recipients will know that the message originated with the holder of the private key. Moreover, if the public key effectively decrypts the message, recipients will know that the message has not been altered. The use of public key cryptography in authentication mode can therefore ensure *authentication* of the identity of the sender and *integrity* of the message. Use of public key cryptography in authentication mode provides the basis for *digital signatures*.

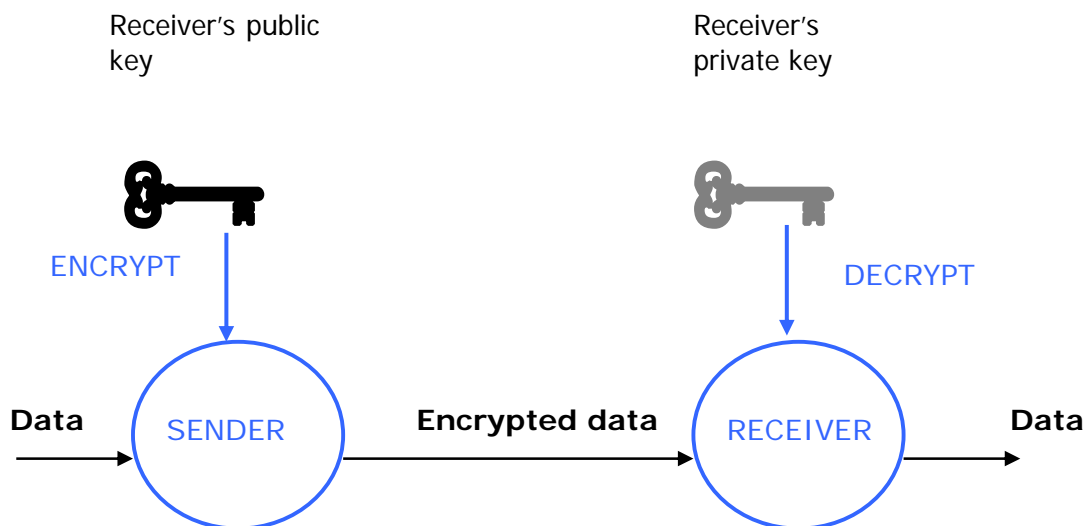


Figure 6.3 - The Asymmetric cryptographic system – encryption mode

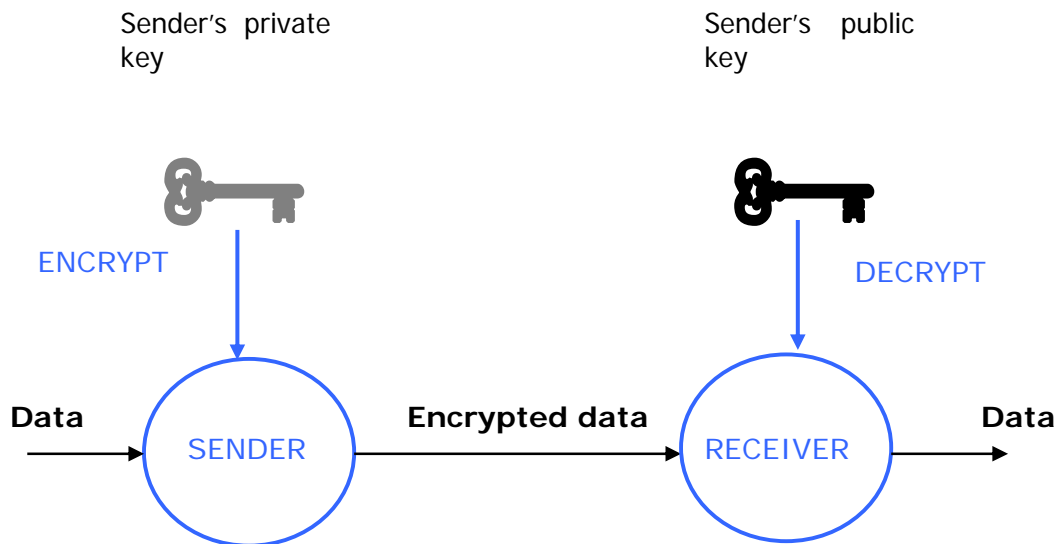


Figure 6.4 - The Asymmetric cryptographic system – authentication mode

(iv) Digital signatures

Encrypting and decrypting an entire message requires substantial processing power. This problem can be addressed by the use of digital signatures. To create a digital signature, a unique value, known as a *hash value* (or message digest), is calculated for a message. The hash value is calculated by means of a mathematical operation, or algorithm, known as a *hash function*. The sender's private key is then used to encrypt the hash value. Digital signatures therefore essentially comprise three main components:

- a public/private key pair;
- a one way hash function; and
- a trustworthy means for publishing public keys.

A recipient who successfully uses a public key to decrypt the message can be sure that it has been sent by the holder of the private key. Moreover, as each message has a unique hash value, if the hash value calculated at the point of reception matches the encrypted hash value, the receiver can be sure that the message has not been altered in transit. Provided that the private key

has not been compromised, digital signatures can ensure authentication of the identity of the sender, integrity of the message and non-repudiation.

Once a digital signature has been created for a message, the sender can use the intended recipient's public key to encrypt the message, including the digital signature. This technique, known as double encryption, can ensure the confidentiality of the message.

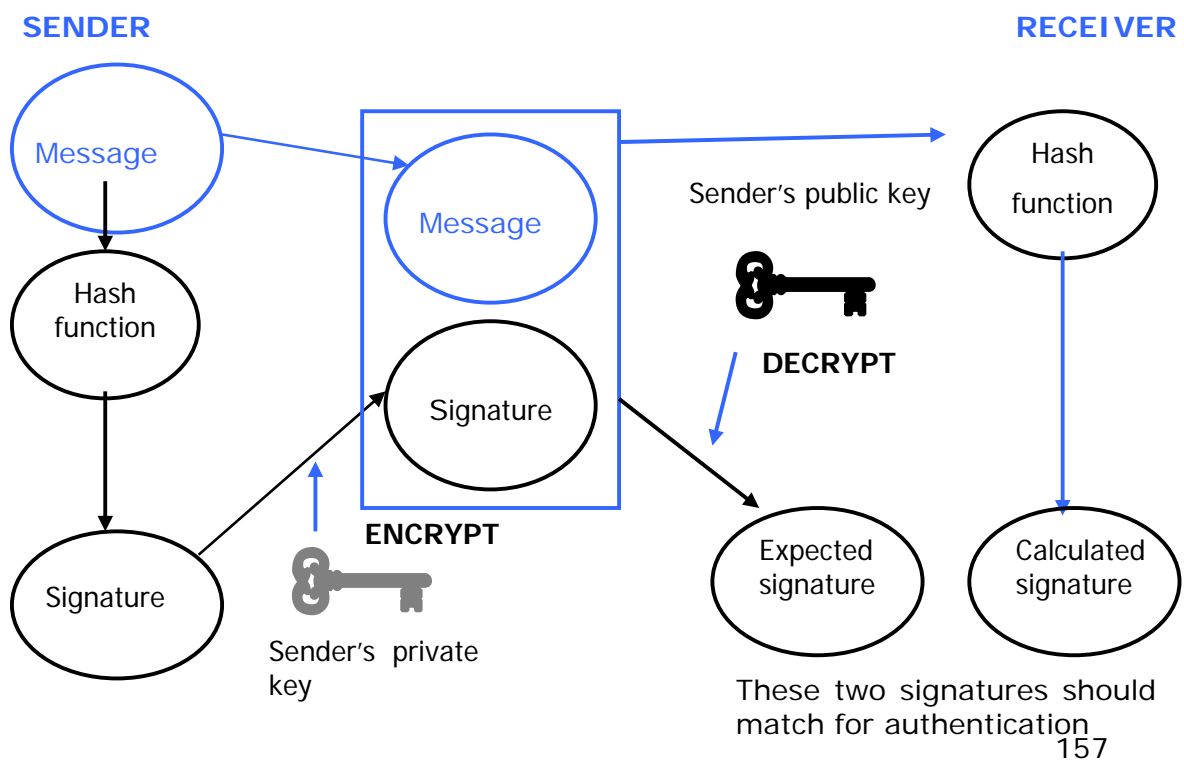


Figure 6.5 - Asymmetric cryptography with digital signature

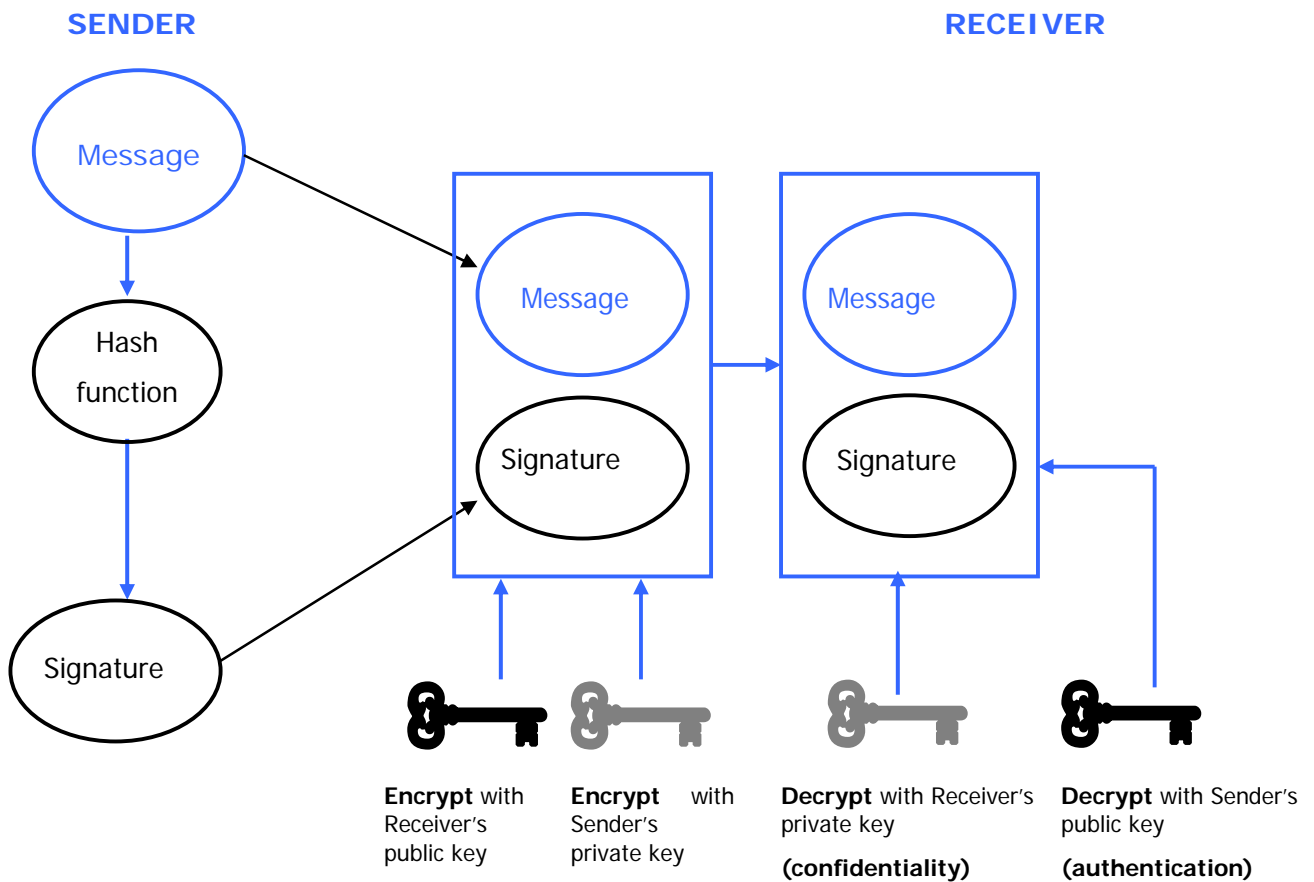


Figure 6.6 - Asymmetric cryptography with digital signature: double encryption

(v) Public Key Infrastructure (PKI)

Public key cryptography depends upon users being able to trust that a public key is, in fact, linked to the legitimate owner of the key pair. It is extremely important that intruders cannot undermine the integrity of a public key by substituting their own key, which would allow encrypted contents to be disclosed and digital signatures to be forged. Trust with unknown entities online is conventionally ensured by relying upon a neutral party who can be trusted, known as a *trusted third party*. The administrative system for ensuring trust in a public key cryptosystem is known as a *Public Key Infrastructure (PKI)*.

The trusted third party in a PKI is known as a Certification Authority (CA). A CA is responsible for issuing *digital certificates*. A digital certificate is created by a user (or subscriber) generating a key pair and sending a request to the CA, together with the user's public key. The CA then authenticates the information, including the identity of the key holder, and issues a certificate, which contains the name of the subscriber, the public key, a certificate serial number, an issuance date and the digital signature of the CA. The CA will create a hash value for the digital certificate and sign it with the CA's private key.

A PKI conventionally consists of the following parties:

- Certification Authorities (CAs), who are responsible for issuing and revoking digital certificates;
- Registration Authorities (RAs), who are responsible for managing interactions between subscribers and CAs, including verifying subscriber information and maintaining reliable lists of digital certificates as well a certificate revocation list (CRL);
- Subscribers (S), who are digital certificate holders; and
- Relying parties (R), who rely on digital certificates to verify a communication.

The effective operation of a PKI depends upon the extent to which a CA can be trusted. The traditional means of ensuring trust in a PKI is a hierarchical system in which trust in a number of CAs is guaranteed by a centralised trusted third party, known as a *Root Certification Authority (RCA)*. An alternative to hierarchical systems of trust are non-hierarchical systems, such as Zimmerman's *web of trust*, which rely upon trusted key pair holders guaranteeing that other key pair holders can be trusted.⁵

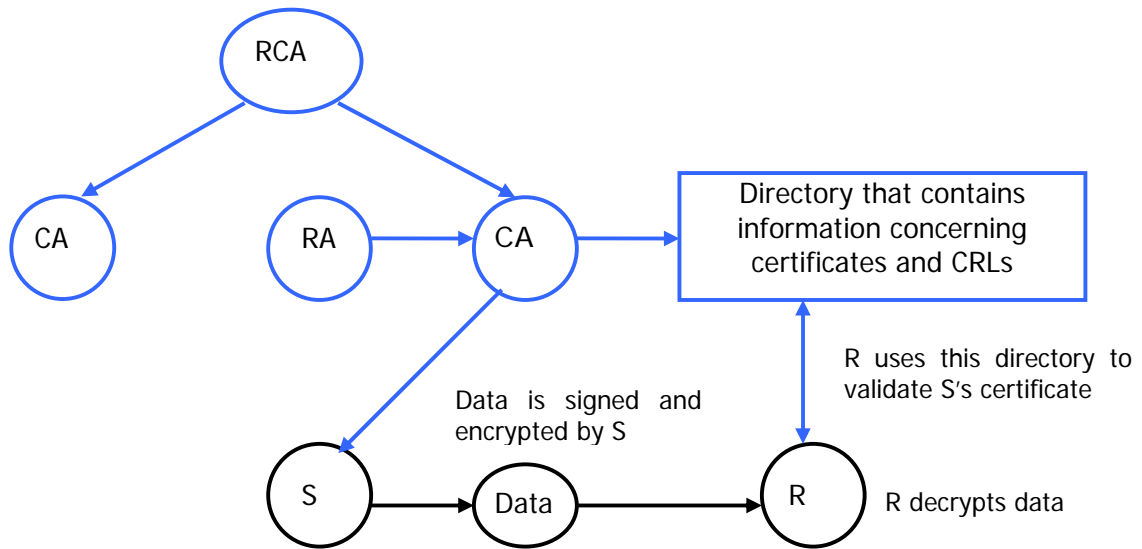


Figure 6.7 - Parties in a hierarchal PKI system

(vi) X.509 Version 3

The most common standard for distributing digital certificates is defined by the IETF/ITU X.509 standard.⁶ The standard requires digital certificates to include the following fields: version number; serial number; CA's signature; issuer; issue and expiration dates; subscriber's name; public key information; issuer's unique identifier; and subscriber's unique identifier. X.509v3, released in 1997, provides for an extensions field that allows for additional information. Additional information can relate to key information; policy information; subscriber and issuer attributes; and certificate revocation lists. An important modification to X.509 made by X.509v3 was the introduction of greater flexibility in the way in which the relationships between CAs may be structured. X.509v3 therefore allows for the interoperation of PKIs that implement different security policies.

(vii) Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) (also known as *Transport Layer Security*, or *TLS*) is the most common information security protocol for TCP/IP (Internet) communications. The SSL protocol provides a 'security handshake' in which computers exchange bursts of information to ensure a secure negotiated session between client and server computers.

SSL works as follows:

- the server computer sends its public key, in the form of a digital certificate, to the client computer;
- the client computer creates a random private key (known as the 'session key') for symmetric cryptography, and encrypts it using the server's public key;
- the session key is a unique symmetric key used only for the particular communications session;
- the server decrypts the message from the client computer using the server's private key to extract the session key;
- the server acknowledges that it has successfully received the session key; and
- subsequent communications between the client and server computers are encrypted using the session key.

As only the server computer has the private key that can decrypt information encrypted with its public key, SSL is used to *authenticate* the server. Moreover, as communications between the client and server are encrypted using the private session key, SSL protects the *confidentiality* and *integrity* of the data exchanged.

Given that most users do not have digital certificates, SSL sessions usually only provide for *server authentication*. In the event that a client has a digital certificate, client authentication is an optional additional feature.

6.4 INFORMATION SECURITY INITIATIVES

This section of the chapter explains particular information security initiatives that are relevant to the DART project. The information security initiatives dealt with build on the information security fundamentals explained immediately above.

6.4.1 Globus Grid Security Infrastructure (GSI)

The *Globus Alliance* is an alliance of organisations and researchers based at Argonne National Laboratory, the University of Southern California's

Information Sciences Institute, the University of Chicago, the University of Edinburgh, the Swedish Center for Parallel Computers, the U.S. National Center for Supercomputing Applications (NCSA) and Univa Corporation.⁷ It conducts research aimed at developing technology, standards and systems for *the Grid*.

The Globus Alliance produces open-source software for Grid applications. The Globus Toolkit® is an open-source software toolkit used for distributed security, resource management, data management, communication, fault detection and portability. The Toolkit is aimed at providing seamless collaboration across high-end computing resources. It allows for seamless remote access to resources while providing for local control of who has access to such resources.

The Globus Toolkit® includes security tools, which provide for authentication and authorisation. The security component of the Toolkit uses *Grid Security Infrastructure (GSI)*, which is based on asymmetric (public key) cryptography. The GSI provides for:

- secure communication (authenticated and perhaps confidential) across a computational Grid;
- security across organisational boundaries; and
- single sign-on (SSO) for users.⁸

The GSI incorporates the following components:

- *digital certificates* which comply with the X.509 standard format;
- *mutual authentication* which uses the *Secure Sockets Layer (SSL)* protocol for an exchange of certificates;
- *password protection* of the user's private key, with a password being required to decrypt the file containing the user's private key. This means that a user must use a password to use the GSI; and
- *delegation capability* which is provided by an extension to the SSL protocol that allows for single sign-on (SSO). *Delegation* means that once a user accesses a remote system, permission is given to the remote system to use his or her credentials to access other systems. Delegation in the GSI involves the use of a proxy, whereby a key pair and digital certificate (the proxy certificate), with limited life-spans, are issued. Once a proxy has been created, the user can use the proxy

certificate and private key for authentication without needing to enter a password more than once.

Confidentiality and information integrity are optional additions to the GSI. While the GSI is to authenticate the identities of users and services, authorisation and access control is left to tools such as *Shibboleth*, which is described immediately below.

The DART project demonstrator models have adopted the standard GSI for authentication purposes. For the purposes of the demonstrator models, the Monash University Certification Authority (CA) will be responsible for issuing digital certificates for the GSI.⁹ It is intended that an AusCERT root CA (RCA) will be incorporated as the RCA for DART resources during the ARCHER phase of the project. This is explained further below in the section of the chapter dealing with the Australian Higher Education *eSecurity Framework*.

6.4.2 Shibboleth

The Shibboleth System is an open-source Internet2 Middleware Initiative (I2MI) that is designed to ensure secure user access to web-based resources among multiple organisations.¹⁰ It conforms to the Security Assertion Markup Language (SAML), which is produced by OASIS, the principal standards body for Extensible Markup Language (XML). Another Australian e-Research initiative, the Meta-Access Management System (MAMS) project, is working on implementing Shibboleth into middleware systems.¹¹

Shibboleth appears to be particularly well-adapted to a university-based e-Research infrastructure, such as DART, as:

- it allows for a single sign-on across multiple organisations;
- which have potentially different authentication technologies and procedures;
- while adequately ensuring secure user access to web-based resources.

The Shibboleth System has two components:

- the Shibboleth Identity Provider (IdP) software; and
- the Shibboleth Service Provider (SP) software.

The typical Shibboleth sign-on process includes the following steps (see Figure 8.8 below):¹²

1. When a user's browser accesses a web resource, the SP software re-directs the user to a navigation page, which lists the organisations authorised to access the resource.
The user selects his or her organisation.
2. The browser is directed to the web-site of the user's organisation that runs the IdP software.
The user signs-on using the sign-on method chosen by his or her organisation. This will usually involve entering a username and password.
3. The IdP software directs the user back to the resource site and sends information establishing that the user has signed-on, which is verified by the SP software.
4. The SP software requests additional information from the IdP software, known as 'attributes', about the user. The user attributes may include information such as that the user is a faculty member or a student. Information about user attributes is essential where different levels of access depend upon characteristics of a user, such as whether the user is a faculty member or a student.
5. The SP software receives the user attributes and the attributes are compared with the Web-site's access policy, whereupon access is either permitted or denied.

As is clear from this process, Shibboleth allows users to access web-based resources across multiple organisations by using a single sign-on (SSO) procedure. Shibboleth adopts the principle of *federated identity* in order to ensure interoperability across organisations that have different authentication and authorisation methods. The principle of federated identity provides for a user's authentication to be recognised across multiple organisations or IT systems.

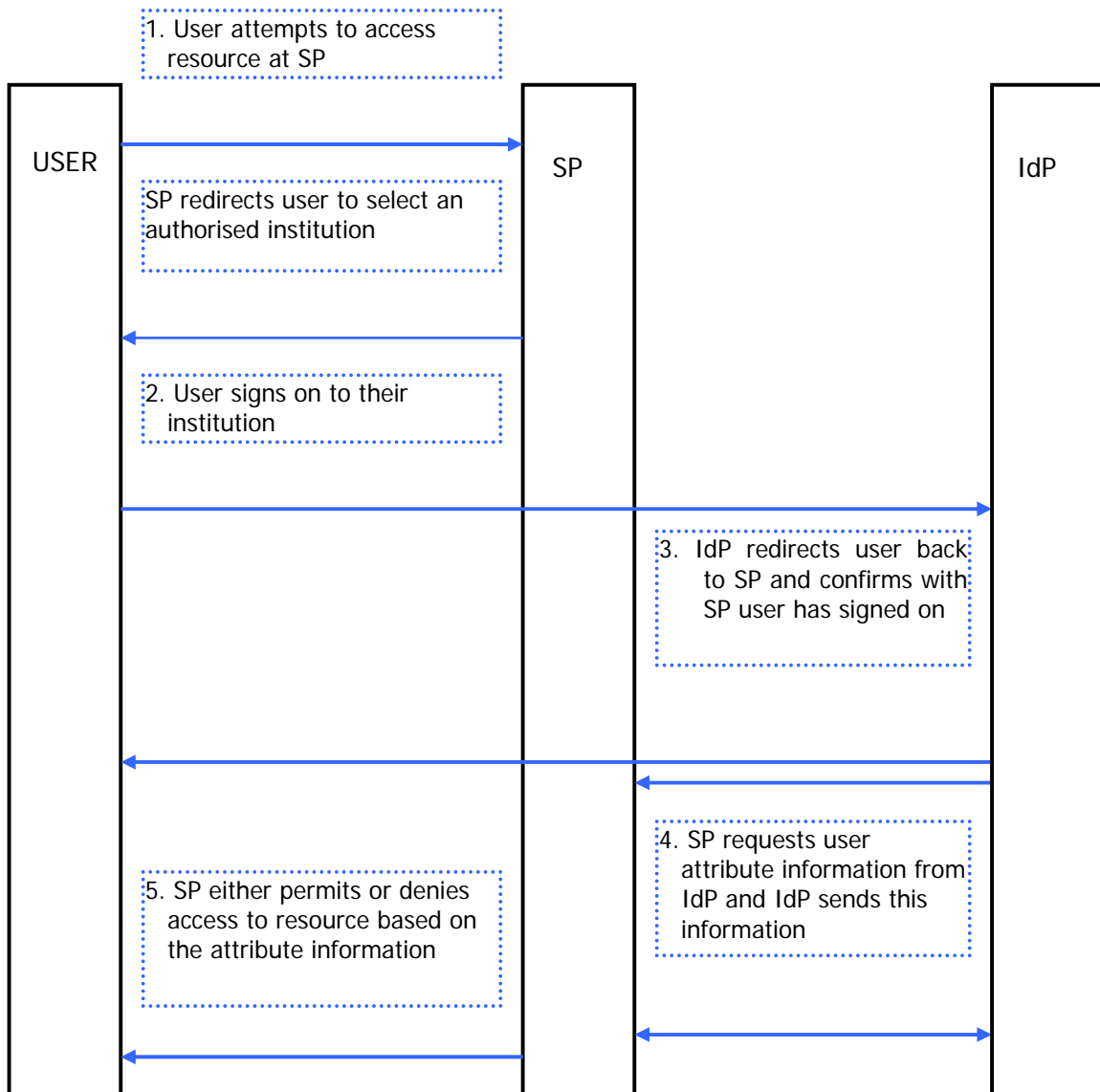


Figure 6.8 - The Shibboleth system¹³

Shibboleth will be incorporated into the DART/ARCHER project upon the successful completion of the MAMS project (described below).

6.4.3 The Australian Higher Education eSecurity Framework

A number of initiatives have been funded to develop a secure environment for on-line collaboration for the Australian Higher Education Sector, while minimising risk to business-like institutions. Two important projects have been:

- *Meta Access Management System Project (MAMS)*, which is aimed at implementing Shibboleth into middleware systems; and
- *CAUDIT (Council of Australian University Directors of Information Technology) PKI Federation Project*, which is aimed at establishing a National Certificate Authority for participating universities. The first phase of this project, the *CAUDIT PKI Federation pilot*, included the development of policies and guidelines, the implementation of a prototype certificate management system and research into interoperation issues.

The *eSecurity Framework* project has been funded to build on these projects to establish a PKI for the Higher Education sector and develop a pilot federation to implement Shibboleth across the sector.¹⁴ The project is led by University of Queensland (UQ), in partnership with Macquarie University, the Council of Australian University Directors of Information Technology (CAUDIT), the Australian Partnership for Advanced Computing (APAC) and AARNet Pty Ltd.

The specific objectives of the *eSecurity Framework* project are:

- *Putting PKI into Production* in the Australian Higher Education sector;
- *Establishing PKI/Shibboleth alignment*, which involves developing a unified model for federation and trust aligning PKI developments, arising from the CAUDIT PKI Federation project, with Shibboleth developments, arising from the MAMs project;
- *Reducing the Systems Cost barriers to entry for PKI*, which involves lowering the barriers to entry to the adoption of PKI by universities by, for example, developing training, documentation and support; and
- *Integrating Grid technologies with PKI/Shibboleth*, which involves integrating the Shibboleth authentication architecture with the APAC Grid infrastructure.

It is envisaged that the Australian Computer Emergency Response Team (AusCERT), which provides security warnings, alerts and advice to Australian universities, will be the centralised root CA (RCA) for the *eSecurity*

Framework. Once the Australian Higher Education sector PKI environment has been established, it is intended that there will be mutual recognition between AusCERT and other RCAs, such as the U.S.'s Higher Education Bridge Certificate Authority (HEBCA) and the Federal Bridge Certificate Authority (FBCA). In pursuit of the above objectives, the Australian higher education Grid, PKI and Shibboleth communities have agreed to form a federation to align their policies and practices, but a name for the federation has yet to be adopted.

The ARCHER phase of DART will use AusCERT as the RCA for access to DART resources. It is intended that the DART project will adopt the approach to certification and identity checking developed by the *CAUDIT PKI Federation* project, including the use of four certification levels.¹⁵ Under this approach different certification levels are used to define the degree of identity checking and verification required to authenticate users according to the requirements of those who control information resources. The baseline identification process is the '100 points' identity system defined in the *Financial Transaction Reports Act 1988* (Cth) and the *Financial Transaction Reports Regulations 1990*, as adapted for the Higher Education sector.

The CAUDIT PKI Certification Levels are set out in **Table 6.1**

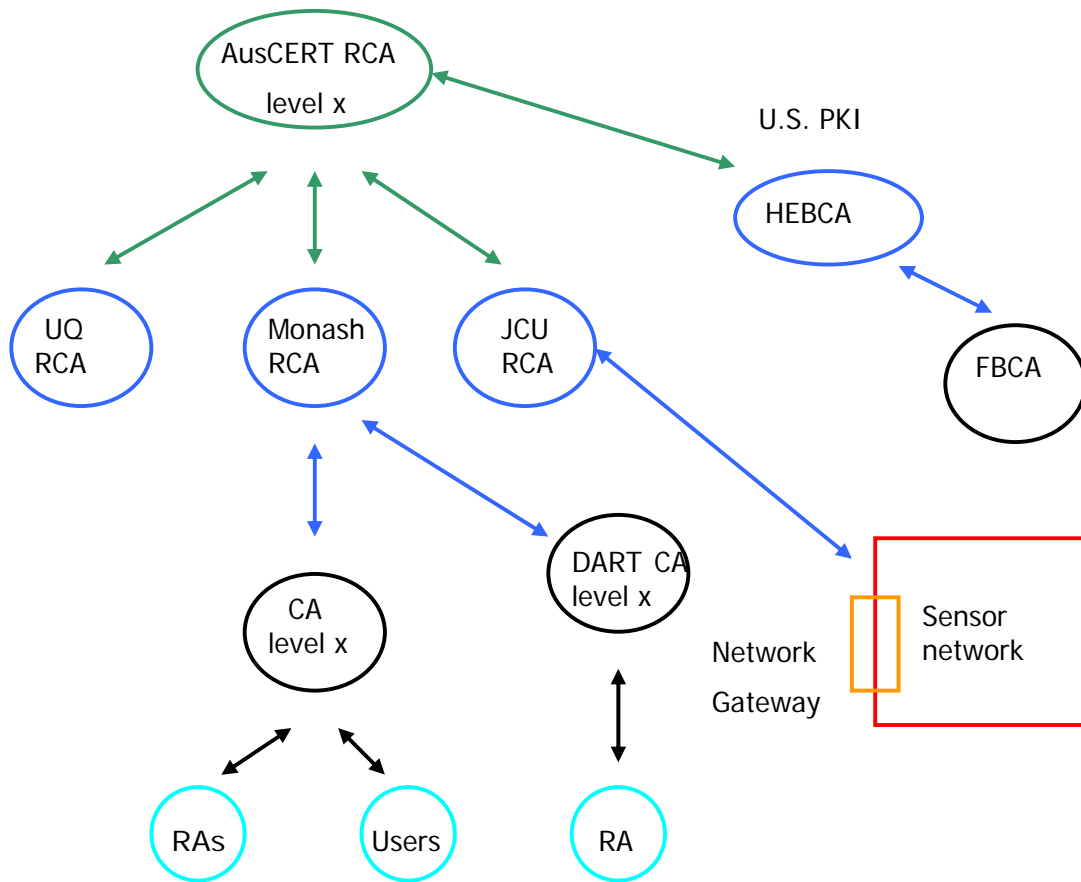
Table 6.1 - PKI Certification Levels

Certification Level	Description
<p>Level 1</p>	<ul style="list-style-type: none"> ▪ No proactive identity check provided to the RA ▪ Identity information provided by a body that the RA has a trust relationship. ▪ Example: A student being enrolled in at least one subject is sufficient for the certificate issuing however identity information has only been supplied by QTAC (or similar state body).
<p>Level 2</p>	<ul style="list-style-type: none"> ▪ Subject must provide proof of identity by appearing IN PERSON at the RA. ▪ Individual cannot provide the required 100 points of identification. ▪ Example: Short term contractors at an institution requiring access to PKI-protected systems whose credentials are insufficient credentials to meet the 100 points check but can provide some

	credentials (eg. Driver's licence, credit card, etc).
Level 3	<ul style="list-style-type: none"> ▪ Subject must provide proof of identity by appearing IN PERSON at the RA. ▪ Individual must accrue at least 100 points of identity. ▪ Example: Foreign staff with valid passports and written references from acceptable referees.
Level 4	<ul style="list-style-type: none"> ▪ Subject must provide the same information for Level 3 certification in addition to character background check. ▪ For example a positive check is also conducted by an appropriate external agency.

The default certification level, Level 3, will require satisfaction of the '100 points' test. It is envisaged that each of the levels will correspond to a different private key for the relevant CA, which will confer different levels of access. For example, a Level 1 identity check may be sufficient for temporary use of grid resources, while Level 4 may be required for grid core administrators that have the highest level of trust. As a guide, most university staff and students should be able to satisfy the '100 points' test. It follows that under the DART project, users with a Level 3 certificate will be denied root access to grid resources.

The DART PKI model is set out in the following diagram.



Note: x represents the certificate level of 1, 2, 3 or 4.

Figure 6.9 - DART PKI model¹⁶

6.5 SECURITY POLICIES AND PROCEDURES

Technological measures for protecting information security must be supported by appropriate security policies and procedures. As with technological measures, security policies and procedures are designed to manage the risk of potential security breaches. Security policies and procedures should be part of an integrated security plan.

Developing a security plan entails the following steps:¹⁷

- Perform a *risk assessment*. This involves compiling an inventory of information resources, assessing points of vulnerability and listing security risks.
- Develop a *security policy*. A security policy should prioritise security risks, identify acceptable targets to be met in managing risks and specify the means to be adopted to appropriately manage security risks.
- Develop an *implementation plan*. This involves specifying the actual steps to be taken to achieve the objectives of the security plan, including identifying the technologies to be implemented and the procedures to be followed.
- Establish a *security organisation or unit*, which has day-to-day responsibility for security policy. The security organisation is responsible for user education and training, and identification of security threats and problems. The security organisation is also responsible for administering:
 - *access controls*, meaning rules about who can gain access to networks and information resources;
 - *authentication procedures*, meaning procedures and technologies for authenticating the identity of those entitled to legitimate access; and
 - *authorisation policies*, meaning rules about the different levels of access permitted for different classes of user.
- Conduct a *security audit*. It is important to implement procedures for ongoing reviews of system security, including ongoing reviews of access logs and regular reports on security problems.

• TIP

No security system is complete without adequate security policies and procedures. If security systems are not followed by all participants, then protection measures will lose their ability to prevent unauthorised access to the relevant systems. Security units must routinely check the adequacy of the security framework through security audits and review of policies.

6.6 PRINCIPLES OF LEGAL LIABILITY FOR INFORMATION SECURITY SYSTEMS AND SECURITY BREACHES

Technological measures for protecting information security, and information security policies and procedures, operate against a *legal background* that governs the relationship of parties involved in online transactions and determines the liability of parties for legally recognised harms, including harms that may result from problems with information security systems and security breaches (see Figure 6.10 below). Information technology professionals involved in establishing information security systems are often insufficiently aware of the importance of the *legal framework* for eSecurity. One of the biggest challenges in managing information security risks in an e-Research infrastructure lies in establishing an appropriate legal framework for protecting information security. Unless an adequate legal framework is established, it will be difficult to build the *trust* among parties that is necessary for the success of an e-Research infrastructure.

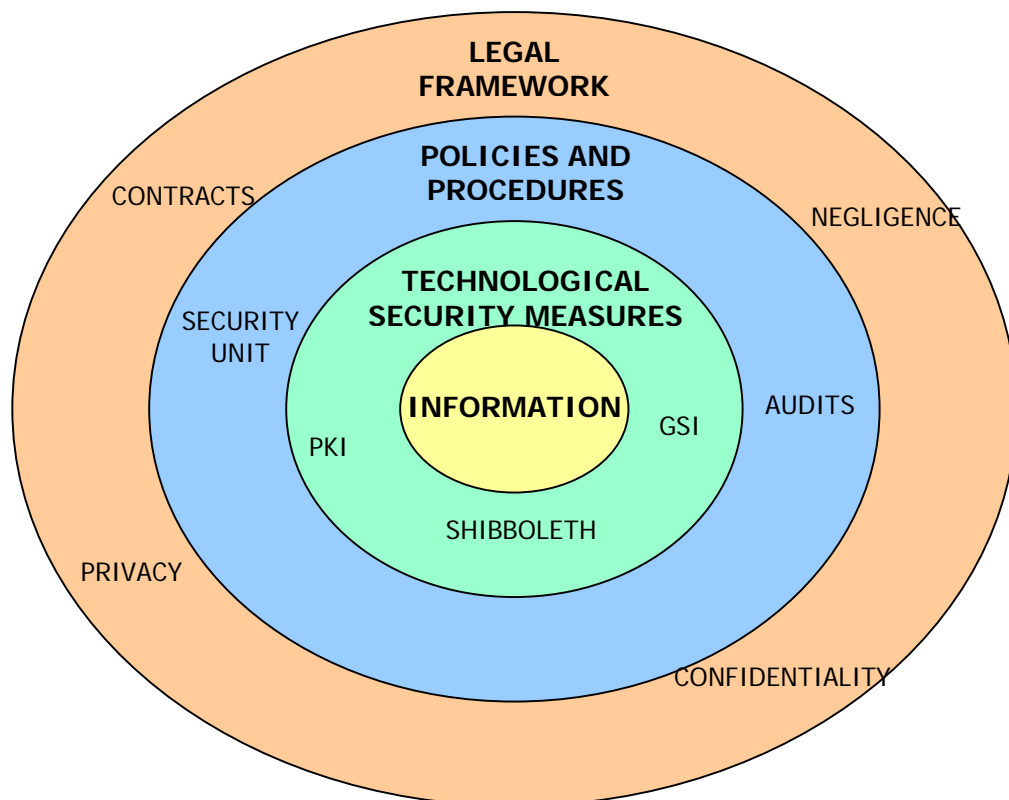


Figure 6.10 - The various elements that influence information security in e-Research¹⁸

The legal framework for regulating information security in the context of an e-Research infrastructure will be established mainly by means of contractual arrangements among parties involved in e-Research transactions. The contractual arrangements should assign responsibility for potential losses incurred from e-Research activities. Drafting the relevant provisions of such contracts necessarily depends upon understanding the sorts of legal liability that may arise from the use of security systems in an e-Research infrastructure.

6.6.1 Participants in e-Research transactions

Before identifying the legal risks arising from the use of e-Research security systems, it is first necessary to identify the participants who may be involved in an e-Research transaction. To simplify, the potential participants in an e-Research transaction may be identified as follows:

- *Authorised Principal (AP)*, who is the person who is authorised to access, use, modify, add to or delete information resources stored on an e-Research repository;
- *Unauthorised User (UU)*, who is not authorised to access, use, modify, add to or delete information resources stored on an e-Research repository;
- *Identity Provider (IdP)*, meaning the entity, such as an AP's university, that is responsible for authenticating the identity or other attributes of an AP;
- *Service Provider (SP)*, meaning the entity that is ultimately responsible for providing access to an information resource in reliance upon the authentication service provided by the *IdP*; and
- The participants of a PKI as described above, which include CAs, RAs, S and R.

This typology of potential users is particularly relevant to security systems that use a distributed authentication and authorisation (or federated trust) model, such as the HERTF. The HERTF uses aspects of both Shibboleth and PKI.

The information that is sent from an IdP to a SP (in relation to systems such as Shibboleth) will commonly include:

- *Authentication statements*, which assert that the AP was authenticated by the IdP using a particular method of authentication; and

- *Attribute statements*, which contain further information needed by a SP, such as whether the AP is a faculty member or a student, which the SP requires before it can make an access control decision.

In addition, the information exchanged between PKI participants will include:

- *Information concerning an entity applying for a certificate*, which will be given by the applicant to the RA and/or CA to authenticate the entity for certificate purposes;
- *Public keys*, which R will obtain from S and the relevant CA to decrypt information encrypted with their respective private keys; and
- *Certificates*, which contain information about S and are signed by a CA. A certificate will be decrypted and relied upon by R to authenticate S. In relation to mutual authentication, both parties will take the role of S and R when authenticating each other. This process will form the basis of a trust relationship between S and R in future communications.

6.6.2 Sources of legal liability

While there have been published studies of the legal liability of parties to electronic transactions using PKI,¹⁹ there have been no published studies of the potential liability of participants in secured e-Research transactions that use distributed authentication systems. This is largely because sophisticated e-Research infrastructures are still in their infancy. Consequently, there remains a degree of uncertainty in relation to the legal liability of participants in e-Research transactions concerning the use of information security systems.

The precise analysis of the liability of participants in e-Research transactions in relation to the use of information security systems necessarily depends upon the particular systems adopted and the particular arrangements between the parties. Nevertheless, the following general sources of potential legal liability may be identified:

- *Breaches of information privacy laws*. Distributed authentication systems may involve the sharing of personal information among independent parties, namely IdPs and SPs. Personal information about a subscriber may also be disclosed during the use of certificates under a PKI. The unauthorised collection, use and disclosure of personal information is dealt with by information privacy laws, which are explained in Chapter 7;

- *Breaches of confidence.* Information stored on e-Research infrastructures may be subject to an obligation of confidentiality. The unauthorised use or disclosure of such information may therefore give rise to actions for breach of confidence. The law relating to breach of confidence is dealt with in Chapter 4;
- *Breach of contract.* Participants in e-Research transactions may be subject to a range of contractual obligations, including those between the parties, or obligations to third parties. Some contractual arrangements may give rise to obligations of confidentiality. Other contracts, including those relating to security systems adopted by the parties, may give rise to a variety of obligations. The potentially unlimited range of contractual obligations that may arise means that this source of legal liability is not readily susceptible to comprehensive analysis;
- *Negligence.* The law of torts refers to civil wrongs developed by the common law which give rise to non-contractual actions against third parties. The best known form of tortious liability is the law of negligence. It is possible to envisage circumstances in which actions in negligence may be brought against APs, IPs, SPs, CAs, RAs and/or Ss in relation to harms arising from unauthorised access, disclosure, modification or deletion of information protected by an information security system. Liability could also arise as a result of an information security system malfunctioning. The legal basis of a negligence action and some examples of potential liability in negligence are discussed below.

6.6.3 Liability in negligence

An action in negligence is available against a person who fails to take reasonable care to avoid foreseeable risks of legally recoverable harm to another.

In order to bring an action in negligence, a plaintiff needs to establish that:

- the defendant owed the plaintiff a duty of care. A duty of care is a legal duty to avoid causing harm that exists where:
 - the harm is reasonably foreseeable; or
 - there is a degree of **proximity** between the defendant and the plaintiff;
- the defendant breached that duty by failing to take reasonable care;
- the breach of duty caused recognisable damage suffered by the plaintiff; and
- the damage was **not too remote** from the breach of duty.

The harms incurred as a result of unauthorised access, or malfunctioning of a security system, will consist of **purely economic losses**, as opposed to physical damage to people or property. Unfortunately, there is considerable uncertainty in the principles that apply to recovery in negligence for purely economic loss. In determining whether an action is available, it is necessary to distinguish the principles that apply to recovery for negligent misrepresentation from the principles that apply to recovery for other acts or omissions that cause purely economic loss.

There is, of course, no general rule that a person has a duty to avoid causing economic harm to another person. On the other hand, it is equally clear that in certain circumstances, it will be possible to recover for purely economic loss. There is, however, no agreement on the principles that apply in determining when a person owes a duty of care to avoid causing purely economic loss to another.²⁰ A duty to avoid causing economic loss may be owed to a class of people, as well as to individuals, provided that the class is sufficiently ascertainable and not indeterminate. Moreover, a person is more likely to owe a duty of care to a vulnerable individual or group who are unable to take reasonable steps to avoid the economic loss.

Liability for economic loss resulting from negligent misrepresentation is a separate area of liability with its own rules. A negligent misrepresentation is an inaccurate or misleading statement of fact, advice or opinion that is made in a business context.²¹ A person who makes such a misrepresentation will be under a duty of care if he or she knew, or ought to have known, that the person who suffers the loss would rely on the representation.²² A person who makes a misrepresentation with the intention of inducing members of a class to rely on the representation will likely owe a duty of care to the members of the class.²³

Examples of potential liability in tort of participants in e-Research transactions

Participants in secure e-Research transactions may potentially incur liability in relation to losses resulting from unauthorised access to information sources. In particular, legally recognised losses may arise from unauthorised use, modification, deletion or disclosure of information protected by a security system. In addition, recoverable losses may be incurred by users who rely upon timely access to essential information resources

The following is a list of examples of possible events that may give rise to liability in tort:

PKI system

- Use of S's certificate to enter into unauthorised communications with R to wrongfully obtain confidential or private information.
- Use of S's private key to intercept, modify or delete information exchanged between S and R
- Inaccurate certification of S's certificate by a CA, which may include:
 - RA's failure to collect adequate or accurate authentication information concerning a body applying for a certificate
 - a failure by the RA and/or CA to update S's authentication information on a certificate;
 - a failure by a CA to alter S's certificate status (suspend/revoke access privileges), after being informed by S that the certificate and/or private key has been compromised.
- Providing improper access to a higher level of information resources, including, for example:
 - inaccurate verification of S's certificate by R; or
 - a CA has incorrectly certified a higher access level for S, which is against the federation's access policy
- Interrupted access to information resources resulting from:
 - delays in a CA certifying a certificate; or
 - the improper suspension or revocation of a certificate.

Shibboleth system

- Use of AP's authentication information, such as a username and/or password, to obtain unauthorised access to an information resource held by SP.
- Incorrect authentication of the AP by the IdP, including, for example:
 - transmission of inaccurate authentication statements or attribute statements to SP;
 - failure to update AP's authentication information;
 - failure to change AP's authentication information, or suspend access privileges, after being informed by an AP that the information has been compromised;
 - incorrect transmission of authentication statements or attribute statements that are associated with a user other than the AP.
- Improper provision of access to information resources by the SP, including, for example:

- inaccurate verification of sign-on information provided by the IdP;
- incorrect provision of access to an information resource where, for example, the user attributes should not allow access to resources of that type in accordance with its access policy.
- Interrupted access to information resources resulting from:
 - faults with authentication processes of IdP; or
 - faults with provision of access by SP.

Summary

There are considerable areas of legal uncertainty in relation to the legal liability of potential participants in e-Research transactions for information security systems, especially the extent to which one participant may be liable to others for its negligent acts or omissions. The allocation of liability between Ss and CAs, APs and IdPs, and between IdPs and SPs, should be dealt with by legally binding agreements between the parties. In drafting provisions allocating liability, it is advisable that the economic principle of imposing liability on the least cost avoider should be adopted. Application of this principle would ensure that liability is imposed on the party that is best placed to prevent economic harms, for example, by adopting adequate security precautions.

Given that there will likely be no relationship between a CA and R, and between an AP and a SP, it would seem to be difficult for liability for economic losses to be allocated by legal agreement between these parties. Moreover, whether an AP owes a duty of care to a SP, or a SP to an AP, is subject to considerable uncertainty. It is possible that, to an extent, the potential liability of these parties could be dealt with by agreement between an IdP and a SP. Over and above this, it may be advisable for parties, particularly Rs and SPs, to take appropriate insurance against liability risks.

6.6.4 Trans-border issues

Given the global nature of e-Research, and emerging e-Research infrastructures, participants in e-Research transactions may not all be located in the one legal jurisdiction. This means that liability disputes may arise between parties that are located in different jurisdictions which have different liability rules. What may generally be referred to as 'jurisdictional issues' are dealt with by a body of law known as *private international law* or *conflict of laws*.

There are three distinct kinds of legal issues that need to be considered in determining where a dispute will be heard, and which laws will apply to the dispute, namely:

- *basic jurisdiction (or inherent power)*, meaning whether the court has power over the parties, or over the dispute;
- *applicable law (or choice of law)*, meaning the law that is to be applied to a multi-jurisdictional dispute; and
- *enforceability of judgments*, once a decision has been made.

Whether or not a court has *basic jurisdiction* over a dispute is determined by the law of the court's own state or country, which is known as the *lex fori*, or the law of the forum. Under Australian law, the most important aspect of basic jurisdiction is known as *personal jurisdiction*, which is sometimes referred to as 'the amenability of the defendant to the writ of the court'. This simply means that the court has power, according to its rules, to apply its processes to a particular defendant. Personal jurisdiction may arise from either common law or statutory rules.

Personal jurisdiction may arise at common law if:

- the defendant is *present* in the jurisdiction at the time of service of the originating process; or
- the defendant *submits* to the jurisdiction of the court.

A defendant is taken to have submitted to the jurisdiction of the court where either:

- the defendant enters an unconditional appearance in an action, meaning that the defendant appears to contest the merits of the case; or
- the defendant has entered a binding contract agreeing to submit disputes to the courts of the forum.

An exclusive foreign jurisdiction clause, meaning a clause requiring disputes to be submitted to the courts of another country, will normally prevent an Australian court from exercising jurisdiction unless there are 'strong reasons to the contrary', such as an inequality of bargaining power.

If personal jurisdiction is not available under the common law rules, a plaintiff will need to rely on statutory rules. All Australian courts have what are known as 'long arm' statutes, established by the relevant court rules, which allow for service of an originating process outside of Australia. There are, however, differences between the detailed rules of the particular courts in Australia as to the procedures and grounds upon which service outside Australia may be granted. Nevertheless, in general terms, some form of nexus or connection is required between the action and the forum before statutory personal jurisdiction will arise. For example, an Australian court will have personal jurisdiction over a defendant in an action in tort, such as an action for negligence, where the tort was committed in the jurisdiction. This means that the relevant acts or omissions must have occurred within the jurisdiction. In some courts, however, there may be personal jurisdiction where a claim is brought in respect of damage suffered wholly or partly in the jurisdiction, regardless of whether the relevant acts or omissions occur in the jurisdiction or elsewhere. Australian courts have held that damage will have been suffered in the jurisdiction where the plaintiff continues to suffer the physical, financial or social consequences of an injury, despite the fact that the injury first incurred outside the jurisdiction.²⁴

Where a defendant has been served with an originating process, he or she may apply to set aside service of the process on the basis that either:

- the claim does not fall within the court rules; or
- the Australian court is 'clearly inappropriate', which is known as the doctrine of *forum non conveniens*.

Once an Australian court has determined that it is able to exercise jurisdiction over a dispute, it is a separate matter to determine the law that is to be applied to the dispute, which is known as *applicable law*, or *choice of law*. The choice of law question is more complex than the question of basic (or personal) jurisdiction, and will often require a detailed consideration of the facts of the particular case. The rules that apply in determining the law to be applied depend upon the nature of the action that is brought by the plaintiff, such as whether the action is in tort or contract.

In the past, the choice of law rules for foreign torts, such as negligent acts or omissions that occur outside of Australia, have been complex and controversial. The law was, however, considerably simplified by the decision of the High Court in *Regie National des Usines Renault SA v Zhang*.²⁵ In essence, *Zhang's case* established that:

- the law of the place where the tort happens, known as the *lex loci delicti*, is the law that will be applied to all cases involving torts committed outside of Australia; but
- Australian courts may grant a permanent stay (halt) to proceedings in cases where it would be contrary to public policy to give effect to the *lex loci delicti*.

The High Court has also recently held that where an Australian court must apply foreign law, the court must, at a minimum, apply the foreign choice of law rules and the laws that these rules yield, which in this case were the laws of Australia.²⁶

It is therefore vitally important to determine the location of the particular acts or omissions that give rise to liability in tort. Despite the simplification achieved by *Zhang's case*, there remain some areas of uncertainty. For example, it is not yet clear whether issues such as the application of limitation periods,²⁷ the kinds of damages that may be recovered and the amount of damages are procedural matters or questions of substance. If these issues are merely procedural, they will be governed by the law of the forum, but if they are considered to be matters of substance, the law of the place where the tort was committed will apply.

The final issue that needs to be considered in relation to trans-border issues is the extent to which an order made by an Australian court is capable of being *enforced* in another jurisdiction. It has been suggested that where a plaintiff seeks an injunction (an order to cease certain behaviour), an Australian court has a discretion to refuse to give the order where enforcing it in a foreign jurisdiction would be difficult.²⁸ In general, however, courts will adopt the view that their orders will not be disobeyed, and will be inclined to grant injunctions, even where it may be difficult to enforce the order.

ENDNOTES

¹ Committee on National Security Systems (U.S.), *National Information Assurance (IA) Glossary* (2006) Instruction No. 4009 <http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf>.

² Bruce Schneier, *Secrets & Lies: Digital Security in a Networked World* (2000).

³ Warwick Ford and Michael S. Baum, *Secure Electronic Commerce* (2000) 97-98.

⁴ The authoritative text on cryptography remains: Bruce Schneier, *Applied Cryptography* (1996). See also: A. Menezes, P. van Oorschot and S. Vonstone, *Handbook of Applied Cryptography* (1996).

⁵ Phil R. Zimmerman, *The Official PGP User's Guide* (1995).

-
- ⁶ Chokhani et al, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* (2003) RFC 3647 <<http://www.ietf.org/rfc/rfc3647.txt>>. X.509 is also known as ISO/IEC 9594-8.
- ⁷ The Globus Alliance, *About the Globus Alliance* (2006) <<http://www.globus.org/alliance/about.php>>.
- ⁸ The Globus Alliance, *Overview of the Grid Security Infrastructure* <<http://www.globus.org/security/overview.html>>.
- ⁹ Monash University, *Monash University Public Key Infrastructure: Certificate Practice Statement* <<http://www.its.monash.edu.au/staff/security/staff-only/certs/cps-v1-1.doc>>.
- ¹⁰ Internet2®, *Shibboleth* (2006) <<http://shibboleth.internet2.edu/>>.
- ¹¹ Meta Access Management System (MAMS), *MAMS Project Overview* (2005) <<http://www.melcoe.mq.edu.au/projects/MAMS/>>.
- ¹² R.L. "Bob" Morgan, Scott Cantor, Steven Carmody, Walter Hoehn and Ken Klingenstein, 'Federated Security: The Shibboleth Approach' (2004) 27(4) *EDUCAUSE Quarterly* <<http://www.educause.edu/apps/eq/eqm04/eqm0442.asp>>. All of the listed sign-on steps are not always required. For example, if a 'cookie' is placed on a user's computer, there may be no need to be directed to the navigation page.
- ¹³ Figure 6.8 is based upon a diagram in: Internet2®, *Shibboleth Architecture, Protocols and Profiles* <<http://shibboleth.internet2.edu/docs/internet2-mace-shibboleth-arch-protocols-latest.pdf>> 7.
- ¹⁴ eSecurity Framework, *Project Update* (2006) <<http://www.caul.edu.au/org/eSecurityFramework2006.pdf#search=%22eSecurity%20Framework%20Project%22>>.
- ¹⁵ Rodney McDuff and Viviani Paz, *CAUDIT PKI Federation: A higher Education Sector Wide Approach* (2006) <<http://middleware.internet2.edu/pki06/proceedings/paz-caudit.pdf>>.
- ¹⁶ Figure 8.9 is based upon work conducted by work package SI4: Zubair Baig, 'An Optimal Public Key Infrastructure for Securing the DART Grid Network' (2006).
- ¹⁷ Kenneth C. Laudon and Carol Guercio Traver, *E-commerce: business, technology, society* (2nd ed, 2003) 285-288.
- ¹⁸ Figure 6.10 is based upon work in: Kenneth C. Laudon and Carol Guercio Traver, *E-commerce: business, technology, society* (2nd ed, 2003) 255, Figure 5.2.
- ¹⁹ Mark Sneddon, *Legal Liability and e-transactions: A scoping study for the National Electronic Authentication Council* (2000) <<http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN014676.pdf>>; C Ellison and B Schneider, 'Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure' (2000) 16(1) *Computer Security Journal* <<http://www.counterpane.com/pki-risks.html>>; Chris Reed, *Internet Law: Text and Materials* (2004) 140-172.
- ²⁰ *Perre v Apand* (1999) 198 CLR 180.
- ²¹ *Hedley Byrne v Heller* [1964] AC 465; [1963] 2 All ER 575.
- ²² *Mutual Life & Citizens' Assurance Co Ltd v Evatt* (1970) 122 CLR 628.
- ²³ *San Sebastian Pty Ltd v Minister Administering Environmental Planning and Assessment Act 1979 (NSW)* (1986) 162 CLR 340.
- ²⁴ *Girgis v Flaherty* (1985) 4 NSWLR 248.
- ²⁵ (2002) 187 ALR 1.
- ²⁶ *Nielson v Overseas Projects Corporation of Victoria Ltd* [2005] HCA 54.
- ²⁷ However, in *Nielson v Overseas Projects Corporation of Victoria Ltd* [2005] HCA 54, the High Court found that the choice of law rules of China provided a discretion to apply Australian substantive law. Therefore, the more generous limitation period in Australia was used.
- ²⁸ See, for example: *Macquarie Bank v Berg* (Unreported, SC NSW, Simpson J, 2 June 1999).

APPENDIX 1

Legal liability of participants in e-Research transactions for information security systems and for security breaches

This section of the chapter introduces a number of specific fact scenarios for examining the legal liability of the various participants in e-Research transactions for information security systems and for losses arising from security breaches. It explains the legal principles that apply to the scenarios where a loss may be incurred as a result of the acts or omissions of one of the participants in an e-Research transaction. As there are a potentially large range of activities that may give rise to issues relating to the allocation of liability between parties, the scenarios are intended to be illustrative only, and are by no means comprehensive.

←TIPS

To avoid uncertainty in relation to the liability of the various participants within e-Research transaction for security, the participants can enter into contractual agreements that set out their respective liabilities under particular circumstances. If such agreements are in place prior to any security breaches, then liability in most cases will be clearly set out in the contract.

PKI

S v R

Scenario 1

An UU uses a S's private key to intercept communications between a S and R. Consequently, the UU causes legal harm by modifying and/or deleting information contained in these communications. The S denies that they are responsible for these actions and denies liability.

Allocating liability in this scenario may be difficult as a S and R may not have previously entered into an agreement that outlines the liability of each party

in relation to certain events. The identity or location of the UU will usually also be difficult to establish.

Assuming that the S can establish that he or she did not commit the relevant actions, then the S may still be liable if:

- The S is responsible for the actions of the UU through the law of agency; or
- The S owes a duty of care to the R to take reasonable care of the S's private key and has acted in breach of that duty, meaning that the R may have an action in negligence against the S.

First, an S may be responsible for any losses incurred by the actions of an UU if the UU is the S's agent, and the UU's actions are within the scope of the agency. An agency is a relationship between one party (the principal) and another party (the agent), where the agent has the authority to act on behalf of the principal so as to affect legal relations between the principal and third parties.¹ An agency relationship may be created by:

- express or implied agreement of the principal and the agent;
- subsequent ratification by the principal of the agent's acts done on behalf of the principal;
- operation of law, such as pursuant to statute; or
- by estoppel, under the doctrine of apparent authority.

An agency by estoppel will arise where the principal, by words or conduct, represents to a third party that a particular person (the agent) is authorised to act for the principal, and the third party acts in reliance on the representation to enter into transactions with the agent. In such circumstances, the principal is 'estopped', or prevented, from denying that there is an agency relationship.

Secondly, if the S has been careless with his or her authentication information, then the S may be liable in negligence for any losses caused by his or her carelessness. As explained above, however, the current Australian law of negligence in relation to recovery for purely economic loss is quite uncertain. The principal difficulty lies in determining whether or not an S will owe a duty of care to a R. Following *Perre v Apand Pty Ltd*,² it appears that a duty of care in relation to economic losses will not be owed to a class, such as the class of Rs, where it is impossible to sufficiently determine the members of the class at the time of the relevant act or omission. In this

scenario, the class of Rs may be ascertainable if it can be established that considering the arrangements and/or understandings between the parties, that S would owe a duty of care to that class. For example, S may regularly use their private key to communicate with certain Rs. Ultimately, if the relevant R is within that class the S may owe them a duty of care.

Example of unauthorised access by UU raised by a demonstrator model

Crystallography demonstrator: A crystallography researcher (S) may employ a research assistant to help them with experiments. The researcher may allow the assistant to use the researcher's private key to conduct communications with others (Rs) within the DART security structure. The assistant however, uses the private key to obtain confidential research information about another R for their own benefit. The R suffers economic losses that are due to the loss of commercial profits that the information would have generated had it been kept confidential. There is no agreement between the S and R in regards to liability. The S may be liable for the actions of the assistant (as an UU), as the S could be seen as the agent of the assistant as they have allowed them to use his or her private key to conduct communications on their behalf. However, the S may not be an agent if it can be established that the assistant was not acting within their job description when they entered into unauthorised communications. Nevertheless, the S may still be liable as they have given the assistant the ability to enter into such communications by giving them their private key.

CA v R

Scenario 2

A S becomes aware that their private key has been compromised and informs the relevant CA within a reasonable time after they have become aware of this. The CA fails to promptly suspend or revoke the S's private key and certificate. An UU uses a S's private key/certificate to pose as S and correspond with R. Consequently, the UU causes legal harm by entering into false agreements with R, or disclosing confidential information contained in communications between S and R ..

In this case, the CA, rather than the S, may be liable for any losses suffered by the R for not altering the status of the S's certificate.

It is unlikely that a CA and R have entered into an agreement establishing legal liability. Nevertheless, the CA may have entered into an agreement with S that may outline the responsibilities of each party. CAs often outline the rights and obligations of each party in their Certification Policies or Certificate Policy Statements. The agreement may outline that the CA is liable to Rs under certain circumstances.

However, if there is no agreement between the CA and S, the R may still be able to bring an action in negligence against the CA. This action may be based upon:

- An act or omission made by the CA that has caused purely economic loss; or
- A negligent misrepresentation made by the CA.

In regards to the first option, whether the R can bring an action against a CA for the recover of purely economic loss will depend upon whether:

- the CA owed the R a duty to take reasonable care in relation to the certificates; and
- the CA committed an act or omission in breach of that duty.

For a CA to owe a duty of care to the class of Rs, the members of the class must be sufficiently ascertainable at the time of the relevant act or omission. Establishing a class of Rs in this case may be difficult, as a S may communicate with many Rs using their private keys, where such communications are not known by the CA. However, if a S regularly communicates with a particular R within a federated system, then the CA may be more likely to owe a duty of care. Nevertheless, it would be difficult to establish a specific class in this scenario.

Assuming that a CA owes a duty of care to the R, a number of considerations may be relevant to determining whether or not there has been a breach of this duty. In this instance, where the CA has failed to take action to suspend or revoke S's certificate, the CA will likely be in breach of its duty. Furthermore, the extent to which the CA has put in place, implemented and followed reasonable security policies and procedures will be relevant in determining whether there has been a breach of duty.

In relation to the second option for the basis of a negligence action, it is possible that an out of date certificate may amount to a negligent misrepresentation. The relevant misrepresentation would be that the S's certificate is still secure and can be relied upon for communications. There may, however, be some uncertainty as to whether automatic transmission of the relevant information from the S and/or CA to the R is a statement (or 'utterance') – in which case there may be an action for negligent misrepresentation – or an 'act' – in which case the action must be brought for a negligent 'act' resulting in economic loss. If the information amounts to a misrepresentation, a CA may owe a duty of care to a R if the CA knew, or ought to have known, that the R would act in reliance on the information. As the certificates provided by CAs are used by Ss to communicate with Rs, CAs would be aware that Rs will rely on information provided by CAs to authenticate Ss. Therefore, a CA may owe a duty to a R to take reasonable care to ensure that the information it provides is accurate. Again, the extent to which a CA has adopted, implemented and followed adequate security policies and procedures will be relevant in determining whether or not there has been a breach of duty.

Example of compromised private key raised by a demonstrator model

Climate research demonstrator: A climate researcher (S) becomes aware that someone has hacked into the file on their computer where their private key is stored. The S informs their CA (eg. Monash CA) that their private key has been compromised. The CA fails to inform the RA of the compromise and to revoke the certificate, as well as placing the certificate on the CRL. Subsequent to the S informing the CA of the compromise, the hacker uses the private key to enter into an unauthorised agreement with a R. Under the unauthorised agreement, the R transfers confidential research information concerning climate models to the UU. The R suffers economic loss due to the disclosure of the research information to another research institution by the UU. There are no contractual agreements between any of the parties. Nevertheless, the CA may be liable to the R for this loss if it can be established that the CA breached their duty of care to the R (as an identifiable member of a class that the S usually communicated with) to ensure that the certificates could be relied upon. The CA may also be liable for misrepresentation as they have inaccurately represented that S's private key is still secure by continuing to certify S.

Shibboleth system

AP v SP

Scenario 3

An UU uses an AP's authentication information (such as the AP's username or password) to obtain unauthorised access to information resources held by a SP and, as a result, causes recognised legal harm by, for example, modifying or deleting information. The AP denies that he or she was responsible for the relevant actions, and denies liability.

There will not usually be a binding agreement between the AP and SP allocating liability between the parties. Moreover, it may not always be possible to locate or confirm the identity of the UU.

Similarly to Scenario 1 above, assuming that the AP can establish that he or she did not commit the relevant actions, then the AP may still be liable if:

- The AP is responsible for the actions of the UU through the law of agency (as discussed above); or
- The AP owes a duty of care to the SP to take reasonable care of the AP's authentication information and has acted in breach of that duty, meaning that the SP may have an action in negligence against the AP.

In relation to liability under negligence, the AP may be liable where they have been careless with their authentication information. However, as discussed above, a duty of care in relation to economic losses can only be established where it is possible to sufficiently determine the members of the class at the time of the relevant act or omission. In this scenario, it is impossible to be definitive about whether the class of SPs is sufficiently ascertainable for there to be a duty of care without additional factual details about the relevant parties, the arrangements between the parties and the understandings of the parties. Nevertheless, if a SP is part of a class that holds information resources that are regularly accessed by APs, then the AP may well owe a duty of care.

Example of compromised private key raised by a demonstrator model

Digital History demonstrator: A researcher (AP) that is responsible for placing women's stories on the Women on Farms website gives an individual their username and password so that the individual can access particular resources for the website so that they can submit and modify their story themselves. The individual however, uses the authentication information makes unauthorised modifications and additions to other individuals' stories archived in the DART repositories, where the privacy of individuals is breached. The individual also makes unauthorised copies of Creative Commons protected work, which breaches copyright. The SP of the website suffers loss as a result of these breaches to copyright and privacy. There are no contractual agreements concerning liability between any of the parties. The researcher that provided the individual (UU) with the ability to make these modifications may be liable to the SP under the law of agency (where AP is the agent of the UU) and/or for breaching their duty to the SP to take reasonable care of their authentication information. The SP in this case would most likely be within an ascertainable class as the AP would regularly use the particular SP to access the website resources.

← TIP

Those that are able to access DART resources through the DART security mechanisms (PKI and Shibboleth) should not disclose their private keys and/or their authentication information to others who are not authorised to access the system.

IdP v SP

Scenario 4

An UU or AP obtains unauthorised access to information resources held by a SP and, as a result, causes recognised legal harm, such as the unauthorised modification or deletion of information. The unauthorised access is obtained as a result of inaccurate authentication statements or attribute statements provided by the IdP to the SP.

As parties to a distributed authentication system, it can be expected that IdPs and SPs will be subject to an overarching legal agreement. It is

expected that such an agreement will deal with the allocation of liability in the event of recognised legal losses.

In the absence of a legal agreement, the SP may be able to bring in action in negligence against the IdP for the recovery of the relevant losses. Similarly to Scenario 2 above, the availability of an action in negligence depends, first of all, on whether the action lies for an act or omission of the IdP that causes purely economic loss, or whether the action is for a negligent misrepresentation made by the IdP.

The ability of a SP to bring an action in negligence against an IdP for the recovery of purely economic loss depends upon:

- whether the IdP owed the SP a duty to take reasonable care in relation to authentication statements and/or attribute statements; and
- if so, whether the IdP committed an act or omission in breach of that duty.

For an IdP to owe a duty of care to the class of SPs, the members of the class must be sufficiently ascertainable. As IdPs and SPs who are part of a distributed authentication system will be in some form of relationship, an IdP is more likely to owe a duty of care to a SP than is an AP. At the same time, the existing degree of uncertainty in this area of the law means that it is impossible to be definitive about whether or not there is such a duty.

If an IdP owes a duty of care to the SP, other considerations need to be taken into account in determining whether there has been a breach of this duty. As discussed above, these considerations can include whether the IdP has failed to take action to correct inaccurate authentication information and whether they have followed suitable security policies and procedures.

In relation to an action for misrepresentation, the relevant misrepresentation would be that the AP's identity has been authenticated (within the IdP's authentication rules) or that an AP has particular attributes (such as that the AP is a faculty member or a student). As with Scenario 2, there be some uncertainty as to whether automatic transmission of the relevant information from an IdP's server to a SP's server is a statement (which may be an action for negligent misrepresentation), or an 'act' (which may be a negligent 'act' resulting in economic loss). If the information amounts to a misrepresentation, an IdP may owe a duty of care to a SP if the IdP knew, or ought to have known, that the SP would act in reliance on the information. Given the objectives and design of distributed authentication systems, it

would seem that IdPs would be well aware that SPs will rely on information provided by IdPs in order to make authorisation decisions in relation to APs. It would therefore seem that an IdP owes a duty to a SP to take reasonable care to ensure that the information it provides is accurate. The implementation of adequate security policies and procedures will also be relevant in determining whether or not there has been a breach of duty.

Example of inaccurate authentication and attribute statements raised by a demonstrator model

Climate research demonstrator: A climate researcher leaves Monash University to work at another research institution. The IdP however, fails to remove their username and password (authentication) from the DART security system. The IdP also fails to update the researcher's attribute statement to say that they are no longer a researcher at Monash University (and unable to access resources via the IdP). The researcher discovers that they are still able to access climate resources from the SP and makes unauthorised copies of confidential climate models stored in DART repositories. The SP suffers economic loss as a result of the disclosure of the research information. There are no contractual agreements establishing liability between the IdP and SP. However, the IdP may be liable to the SP if the IdP is found to have breached their duty of care to the SP to ensure that the authentication and attribute statements could be relied upon. The SP would most likely be a member of an ascertainable class that the IdP would owe a duty of care to as the IdP would regularly be communicating with the SP in relation to these statements. The CA could also be liable for misrepresentation as they have inaccurately represented that the past researcher is still authorised by the IdP as a member of Monash University to access the SP's resources, and can be trusted.

AP v IdP

Scenario 5

An AP has a commercial research contract in which time is of the essence. As a result of an act or omission of an IdP, the identity of the AP is unable to be authenticated in a timely fashion, meaning that the AP is denied access to an essential information resource held by a SP. The AP fails to complete its contractual obligations on time, suffering resulting economic loss.

An AP will almost always have a legally binding agreement with an IdP, which may deal with liability for losses incurred as a result of acts or omissions. The agreement may, for example, specify that the liability of an IdP is limited

provided that it takes certain precautions, such as following relevant security policies and procedures.

In the absence of an agreement, it is likely that an IdP will owe a duty of care to an AP. As the IdP will have an ongoing relationship with an AP, the IdP should be able to reasonably foresee that an AP could suffer economic loss as a result of negligent acts or omissions committed by the IdP. The extent to which the IdP adopts, implements and follows adequate security policies and procedures will be relevant in determining whether there has been a breach of duty.

As the liability of an IdP to an AP for negligent acts or omissions may be dealt with by an agreement between the parties, it is important to understand that there may be legal limits on the extent to which an IdP may seek to limit liability. For example, given the potential power imbalance between an IdP and APs, it may be unconscionable (or 'unfair') for an IdP to include a provision that attempts to excuse it from liability for any acts or omissions whatsoever.

Example of delay in authentication by an IdP raised by a demonstrator model

Crystallography demonstrator: A crystallography department at JCU enters into a contractual agreement with a commercial drug company to conduct experiments for the company to discover the structure of a particular protein that will assist in the development of a new drug. The company wants the work done quickly as they want to patent the drug before their competitors. The crystallography department agrees to conduct the experiments within a certain timeframe. The crystallography researchers need to conduct these experiments using the CIMA architecture, which is accessible through the DART CIMA portal. However, the IdP for JCU has mistakenly deleted the authentication information for the relevant researchers in the laboratory and the researchers are denied access to CIMA. Ultimately, the research is not conducted within the required timeframe and the researchers lose the economic benefits of completing the contract. Even though there is no contractual agreement between the researchers (as AP) and the IdP, the IdP would most likely be liable for the economic loss suffered by the AP as it has breached its duty of care to the AP to ensure that the AP is authenticated and able to access the relevant resources. As the negligent act committed by the IdP involves their mistaken deletion of the AP from the system, then the relevant security policies and procedures of the AP would be irrelevant in this case.

¹ *International Harvester Co of Australia Pty Ltd v Carrigan's Hazeldene Pastoral Co* (1958) 100 CLR 644.

² (1999) 198 CLR 180.

APPENDIX 2

Glossary

Term	Definition
actuator	<p>An 'actuator' is a 'mechanism that causes a device to be turned on or off, adjusted or moved.' For example, a mechanism and motor on a disk drive or the arm of a robot is referred to as an actuator:</p> <p>PCMag.com, <i>Definition of: actuator</i> (2006) http://www.pcmag.com/encyclopedia_term/0,2542,t=actuator&i=37479,00.asp.</p>
agent	<p>An 'agent' is an entity that is authorised to act on behalf of another. In technological terms, an agent is a 'software routine that waits in the background and performs an action when a specified event occurs.' For example, an agent may send a file on the first day of every month: Answers.comTM, <i>agent</i> (2006) http://www.answers.com/topic/intelligent-agents>. There are a variety of forms of agents in technology, such as software agents and intelligent software agents: David Wallace Croft, <i>Intelligent Software Agents, Definitions and Applications</i> (1997) http://alumnus.caltech.edu/~croft/research/agent/definition/>.</p>
archives/public records legislation	<p>Legislation concerning archives and public records governs the management of public records and the preservation of older documents. For a summary of the relevant laws, see Table 7.11, Chapter 7 of this report.</p>
blog	<p>'Blog' is short for Weblog, a web-based journal 'that is frequently updated and intended for general public consumption': bytown internet, <i>Glossary</i> (2006) www.bytowninternet.com/glossary>.</p>
charge-coupled device (CCD)	<p>A 'charge-coupled device' (CDD) is an image sensor that can be used to store information, transfer electrical charge, or create images of objects:</p> <p>Courtney Peterson, <i>How It Works: The Charged-Coupled Device, or CCD</i> (2001)</p>

Term	Definition
	<p><http://www.jyi.org/volumes/volume3/issue1/features/peterson.html>.</p>
climate research	<p>'Climate' is defined as the average weather conditions over at least a thirty year period: Climate Prediction Center, <i>Climate Glossary</i> (2004) <http://www.cpc.noaa.gov/products/outreach/glossary.shtml#C>.</p> <p>The DART project has a number of climate research demonstrator projects that will be used to demonstrate how the DART project can benefit climate research.</p>
confidential information	<p>'Confidential information' is information that can only be used or disclosed in a particular manner. Confidential information is generally information that is not in the public domain: <i>Coco v A N Clark (Engineers) Ltd</i> [1969] RPC 41 at 47; <i>Moorgate Tobacco Co Ltd v Philip Morris Ltd (No 2)</i> (1984) 156 CLR 414 at 437-8.</p> <p>A duty to keep information confidential can be imposed under either contract or equity (see Chapter 6).</p>
copyright	<p>'Copyright' refers to the rights in creative ideas that have been expressed in a material form (for example, in writing). Copyright only provides protection in relation to the expression of an idea (for example, a book or a drawing), rather than the idea itself. Copyright in Australia is governed by the <i>Copyright Act 1968</i> (Cth), which provides copyright owners, or those authorised by the copyright owner, exclusive rights to do or prohibit certain acts in relation to the copyright material (see Chapter 6).</p>
cyberinfrastructure	<p>The term 'cyberinfrastructure' is commonly used in the U.S. to refer to a computing infrastructure that brings remote computer resources together: Chaitan Baru, <i>What is Cyberinfrastructure?</i> (2005) 3 <http://www.geongrid.org/presentations/sacnas2005/sacnas_baru.ppt>.</p> <p>Cyberinfrastructure has been defined as 'a system that: coordinates resources that are not subject to centralized control; using standard, open, general-</p>

Term	Definition
	<p>purpose protocols and interfaces; to deliver nontrivial qualities of service':</p> <p>Ian Foster, 'What is the Grid? A Three Point Checklist' (2002) 1 No. 6 <i>Grid Today</i> http://www.gridtoday.com/02/0722/100136.html >.</p> <p>The term draws an analogy with physical infrastructures such as roads and power grids that support modern society:</p> <p>D Hart, 'National Science Foundation Releases New Report from Blue-Ribbon Advisory Panel on Cyberinfrastructure' (2003) NSCA News http://access.ncsa.uiuc.edu/Releases/03Releases/02.03.03_National_S.html >.</p> <p>The term 'grid' is used in the U.K. to refer to this concept (see below).</p>
digital history	<p>In relation to the DART project, this term refers to projects that concern the digitilisation of historical information. The DART project has three separate digital history demonstrator projects that will highlight how the DART project can be used in the humanities disciplines.</p>
digital signatures	<p>'Digital signatures' are used by those sending messages to verify that they are the entity that sent the message. The recipient of the message can decrypt the message and signature to verify the sender. If the sender also encrypts the message and signature with the recipient's public (publicly known) key, the confidentiality of the message can be ensured.</p>
encryption	<p>'Encryption' is a technological means of protecting information. The process involves transforming intelligible data, known as plaintext, into unintelligible data, known as ciphertext. There are two types of encryption systems (cryptosystems): symmetric (or private key) cryptography and asymmetric (or public key) cryptography. A key is an apparently random series of bits that is used by a cryptographic algorithm. Symmetric cryptography involves using the same key to encrypt and decrypt a message. Asymmetric cryptography involves using a public (publicly known) and private (secret) key. These two keys are known as a key pair.</p>

Term	Definition
e-Research	<p>'e-Research' refers to a new breed of research techniques that use a wide variety of advanced ICT capabilities and research methodologies:</p> <p>Department of Education, Science and Training, <i>e-Research</i> (2005) http://www.dest.gov.au/sectors/research_sector/policies_issues_reviews/key_issues/e_research_consult/default.htm >.</p> <p>e-Research is collaborative and allows researchers to work together across institutional and jurisdictional boundaries. Furthermore, it provides users with an efficient way to manage and use data and information.</p>
e-Science	<p>The term 'e-Science' is often used interchangeably with 'e-Research' and refers to scientific research that is conducted via e-Research techniques. e-Science is usually performed by distributed global collaborations via ICTs, and often requires access to large data collections, large scale computing resources and high performance visualisation for users: National e-Science Centre, <i>Defining e-Science</i> (2006) http://www.nesc.ac.uk/nesc/define.html >.</p>
e-Social Science	<p>'e-Social Science' can be described as social science research that utilises e-Research techniques, such as grid computing: Answers.com™, <i>E-Social Science</i> (2006) http://www.answers.com/topic/e-social-science-1?hl=social&hl=science >.</p>
Freedom of Information (FOI) legislation	<p>Freedom of Information (FOI) legislation refers to the Acts enacted by the Commonwealth and all the Australian States and Territories that govern access by the public to documents (including electronic records) held by public sector agencies. This legislation also allows members of the public to make a request to an agency to amend their personal records if they are out of date, misleading or incorrect (see Chapter 7).</p>
goniometer	<p>A 'goniometer' is 'an instrument that either measures angles or allows an object to be rotated to a precise angular position': Wikipedia, <i>Goniometer</i> (2006)</p>

Term	Definition
	<p><http://en.wikipedia.org/wiki/Goniometer>.</p>
grid	<p>The term 'grid' refers to the computing model that uses the resources of various separate computers that are connected to a network to obtain high levels of computational power and data processing:</p> <p>Answers.com™, <i>Grid Computing – wikipedia definition</i> (2006)</p> <p><http://www.answers.com/main/ntquery?method=4&dsid=2222&dekey=Grid+computing&gwp=8&curtab=2222_1&linktext=Grid%20Computing>.</p> <p>As with the term 'cyberinfrastructure', the 'grid' makes an analogy with the electricity power grid, where computational resources, data and instruments are considered the utilities that can be delivered over a network:</p> <p>P Hobson (2004), 'From Computing to the Power Grid' (2004) 20 <i>Frontiers</i></p> <p><http://www.pparc.ac.uk/frontiers/archiveText/update.asp?id=20U6&style=update>.</p>
information security	<p>'Information security' concerns the protection or safeguarding of information or data. This protection or safeguarding is generally implemented through the protection of information systems. (See 'Information systems security' below)</p>
Information Society	<p>'Information Society' refers to the concept where ICTs are becoming increasingly important to the economic, social and educational goals of society. Therefore, this idea gives rise to the need for increased access to ICTs for all members of the community.</p>
information systems security	<p>'Information systems security' can be described as 'the protection of information systems against unauthorised access to or modification of information ... and against denial of service to authorised users':</p> <p>Committee on National Security Systems (U.S.), <i>National Information Assurance Glossary</i> (2003) Instruction No. 4009.</p>
intellectual property (IP)	<p>'Intellectual property' refers to a group of rights that provide protection to intellectual and creative effort:</p>

Term	Definition
	<p>Peter Butt (ed), <i>Butterworths concise Australian legal dictionary</i> (3rd ed, 2004).</p> <p>This group includes rights provided under the areas of copyright, patents, designs, trade marks, circuit layouts, plant breeder's rights and the equitable doctrine of breach of confidence.</p>
Knowledge Society	<p>The term 'Knowledge Society' is related to 'Information Society'. Knowledge Society is used to highlight the idea that society's most valuable asset is its investment in intangible, social and human social capital, where the most important aspects are knowledge and creativity:</p> <p>European Commission, <i>Knowledge Society – Homepage</i> (2006)</p> <p><http://europa.eu.int/comm/employment_social/knowledge_society/index_en.htm>.</p>
metadata	<p>'Metadata' literally means 'data about data' and can be defined in regards to web-design as 'machine understandable information about web resources or other things':</p> <p>T Berners-Lee, <i>Metadata Architecture</i> (1997)</p> <p><http://www.w3.org/DesignIssues/Metadata.html></p> <p>. Metadata allows users to locate what they specifically require from a vast amount of information.</p>
metadata schema	<p>A metadata schema is a plan that sets out the specifications for the content and structure of metadata. Numerous metadata schemas have been established by those dealing with metadata.</p>
middleware	<p>'Middleware' can be defined as the software services and tools that allow the linkage of information/data resources and computing capability from various sources:</p> <p>Department of Education, Science and Training, e-Research Coordinating Committee, <i>An E-Research Strategic Framework, Discussion Paper</i> (2005) 14</p> <p><http://www.dest.gov.au/sectors/research_sector/policies_issues_reviews/key_issues/e_research_consult/discussion_paper.htm>.</p>
ontology	<p>An 'ontology' in relation to computer science is a description of the relationships and concepts that can exist for an agent or a community of agents</p>

Term	Definition
	<p>(see 'agent' above). An ontology is usually written as a set of definitions of formal vocabulary.</p> <p>Ontologies usually describe: individuals (basic or ground level objects), classes (collections, sets or types of objects), attributes (features, characteristics, properties or parameters that objects may have and share) and relations (ways that the objects can relate to each other): Wikipedia, <i>Ontology (computer science)</i> (2006) <http://en.wikipedia.org/wiki/Ontology_%28computer_science%29>.</p>
open access	<p>'Open access' refers to digital content, such as scientific or scholarly journal articles, that is freely available online: Wikipedia, <i>Open access</i> (2006) <http://en.wikipedia.org/wiki/Open_access>. The Berlin Declaration on Open Access to Knowledge in the Sciences and Humanities is a major international initiative concerning open access. This Declaration defines open access as a 'comprehensive source of human knowledge and cultural heritage that has been approved by the scientific community' that relies, to an extent, on academic community standards to ensure open access to research resources:</p> <p>E Hoorn, 'Repositories, Copyright and Creative Commons for Scholarly Communication' (2005) 45 <i>Ariadne</i> <http://www.ariadne.sc.uk/issue45/hoorn/>; Max Planck Society, <i>Conference on Open Access to Knowledge in the Sciences and Humanities</i> (2006) <http://www.zim.mpg.de/openaccess-berlin/berlindeclaration.html>.</p>
patents	<p>'Patents' are an area of intellectual property (see 'intellectual property' above) and provide a statutory monopoly for new and inventive processes or products that are useful.</p>
plone	<p>Plone is a web content management system that can be used for project groups, web sites, communities, intranets and extranets: Plone™, <i>What is a Plone?</i> (2006) <http://plone.org/about/plone/>.</p>
pre-processing	<p>Under the DART project 'pre-processing' refers to the process of integrating, refining, integrating and</p>

Term	Definition
	<p>storing real-time data streams from sensors and instruments in DART secondary level repositories for processing and data analysis by higher layers of the DART architecture:</p> <p>The DART Project, <i>DART Project Objectives – revised</i> (2006) Internally distributed document.</p>
privacy	<p>‘Privacy’ concerns the desire to be separate or individual and has been described as ‘the condition of an individual when he is free from interference with his intimate personal interests by others’: W L Morison, <i>Report on the Law of Privacy to the Standing Committee of Commonwealth and State Attorneys-General</i>, Report No 170/1973 (1974), [1].</p> <p>Privacy comes in many different forms, such as information privacy and privacy from surveillance. Privacy is protected under various pieces of legislation in Australia (see Chapter 7).</p>
public key infrastructure (PKI)	<p>A ‘public key infrastructure’ (PKI) is a system by which users can rely upon a set of key pairs to send or receive encrypted messages. Key pairs are a set of public and private keys, where the public key is known to the public, while the private key is only known to the owner of the key pair. A person relying upon a key pair (relying party) owned by an entity can confirm its authenticity by checking the digital certificate created by a Certification Authority for the key pair.</p>
real-time	<p>‘Real-time’ in terms of computing means ‘occurring immediately’, or very fast after a stimulating event. Real-time is used to describe various computer features. As an example, real-time operating systems are systems that respond immediately, or very quickly, to input:</p> <p>Webopedia, <i>real time</i> (2006) http://www.webopedia.com/TERM/R/real_time.html.</p>
tagging	<p>‘Tagging’ involves using a metatag – html code to provide keywords and a description for a particular webpage: Wikipedia, <i>Meta element</i> (2006) http://en.wikipedia.org/wiki/Meta_tag.</p>
X-ray	<p>X-ray crystallography is a research technique that is used to determine the structure of molecules, such</p>

Term	Definition
crystallography	<p>as proteins, DNA and inorganic compounds. The technique involves creating a crystal of the relevant substance and targeting this crystal with X-ray beams. The diffraction pattern of the X-ray beams can be used to determine the structure of the substance:</p> <p>Giacovazzo <i>et al</i>, <i>Fundamentals of Crystallography</i> (1992) Preface.</p> <p>The DART project has X-ray crystallography demonstrator projects at each of the three partner institutions.</p>
Weblog	See the definition of 'blog' above.
Web portal	<p>A 'Web portal', or 'portal' is a Web site or service that provides a variety of services and resources, such as search engines and email: Wikipedia, <i>Web portal</i> (2006)</p> <p><http://en.wikipedia.org/wiki/Web_portal>.</p>
Wiki	<p>A 'Wiki' is a type of website that allows users to add and edit content easily and is particularly suited for collaborative writing: Wikipedia, <i>Wiki</i>, (2006)</p> <p><http://en.wikipedia.org/wiki/Wiki>.</p>

APPENDIX 3

Acronyms and Research Initiatives

Initials	Full Text
AA	Annotation and Assessment (a group of DART work packages).
AIMS	Australian Institute of Marine Science: Australian Institute of Marine Science, <i>About AIMS</i> (2006) < http://www.aims.gov.au/ >.
AP	Authorised Principal.
ARCHER	Australian ResearCH Enabling enviRonment project. This project is funded by the Australian Department of Education, Science and Training and will build upon the work completed in the Dataset Acquisition, Accessibility, and Annotation e-Research Technologies (DART) and Australian Research Repositories Online to the World (ARROW) projects: Australian ResearCH Enabling enviRonment (ARCHER) project, <i>Australian ResearCH Enabling enviRonment (ARCHER) project</i> (2006) < http://www.auscope.org/archives/ARCHER%20Background.pdf >.
ARROW	Australian Research Repositories Online to the World project. This project is funded by the Australian Department of Education, Science and Training and is developing policy templates and software solutions to enhance the deposit of and access to published articles in institutional repositories: ARROW, <i>Welcome</i> (2006) < http://arrow.edu.au >.
AusCERT	Australian Computer Emergency Response Team: AusCERT, <i>Profile</i> (2006) < http://www.auscert.org.au/ >.
Australian Higher Education eSecurity Framework	eSecurity Framework, <i>Project Update</i> (2006) < http://www.caul.edu.au/org/eSecurityFramework2006.pdf#search=%22eSecurity%20Framework%20Project%22 >.

Initials	Full Text
CA	Certification Authority.
CA*net4	Government of Canada, <i>Achieving Excellence: Investing in People, Knowledge and Opportunity</i> (2002) Section 3 Government Support for Innovation – 1995-2001- Canada's Innovation Strategy < http://www.innovationstrategy.gc.ca/gol/innovation/site.nsf/en/in04158.html >.
CAUDIT	Council of Australian University Directors of Information Technology: CAUDIT, <i>Home</i> (2006) < http://www.caudit.edu.au/ >.
CISTI	Canada Institute for Scientific and Technical Information: Canadian Institute for Scientific and Technical Information, <i>Welcome</i> (2006) < http://cisti-icist.nrc-cnrc.gc.ca/cisti_e.html >.
CC	Creative Commons project: Creative Commons, <i>Learn More about Creative Commons</i> (2006) < http://creativecommons.org/learnmore >.
CCP4	Collaborative Computational Project Number 4 in Protein Crystallography: CCLRC, CCP4 (2006) < http://www.ccp4.ac.uk/about.php >.
CIMA	Common Instrument Middleware Architecture: instrument-middleware.org, <i>CIMA</i> (2005) < http://www.instrumentmiddleware.org/metadot/index.pl?iid=2119&isa=Category >.
CR	Content and Rights (A group of DART work packages)
DA	Discovery and Access (A group of DART work packages)
DART	Dataset Acquisition, Accessibility, and Annotation e-Research Technologies project. This project, which is funded by the Australian Department of Education, Science and Training, aims to provide the necessary tools for the secure creation, collection, annotation and sharing of digital research data across institutions: DART, <i>Welcome</i> (2006) < http://www.dart.edu.au/ >.
DEST	Department of Education, Science and Training, see: Department of Education, Science and

Initials	Full Text
	Training, <i>Welcome to the Department of Education, Science and Training</i> (2006) < http://www.dest.gov.au/ >.
Digital Library for Earth Science Education	Digital Library for Earth Science Education, <i>What's New at DLESE</i> (2006) < http://www.dlese.org/library/ >.
DMQ	Data Collection, Monitoring and Quality Assurance (a group of DART work packages).
eBank UK project	UKOLN eBank UK Project, <i>Home</i> (2006) < http://www.ukoln.ac.uk/projects/ebank-uk/ >.
EDUCAUSE	EDUCAUSE, <i>What is EDUCAUSE?</i> (2006) < http://www.educause.edu/content.asp?PAGE_ID=720&bhcp=1 >.
Érudit	Érudit, <i>Journals</i> (2006) < http://www.erudit.org/en/revue/index.html >.
e-Science programme	Research Councils UK, <i>About the UK e-Science Program</i> (2004) < http://www.rcuk.ac.uk/escience/default.htm >.
e-Social Science program	The National Centre for e-Social Science (NCeSS), <i>Welcome to the National Centre for e-Social Science</i> (2006) < http://www.ncess.ac.uk/events/conference/2005/panels/collaboration/ >.
EGEE	Enabling Grids for E-science project: EGEE, <i>Welcome to EGEE</i> (2006) < http://public.eu-egee.org/ >.
FRODO	Federated Repositories of Online Digital Objects projects, see: Department of Education, Science and Training, <i>ARIIC Projects</i> (2005) < http://www.dest.gov.au/sectors/research_sector/policies_issues_reviews/key_issues/australian_research_information_infrastructure_committee/ariic_projects.htm >.
Fedora	Fedora, <i>Fedora Digital Repository System</i> (2006) < http://www.fedora.info/documents/brochure/Fedora%20Page%20Final.htm >
FOI	Freedom of Information (see description above in Glossary of Terms).
GÉANT and GÉANT2	GÉANT, <i>Welcome to the GÉANT Website</i> (2005) < http://www.geant.net/ >; GÉANT2, <i>Welcome to the GÉANT2 Website</i> (2006)

Initials	Full Text
	< http://www.geant2.net/ >.
GFarm	Grid Datafarm, <i>Gfarm file system</i> (2006) < http://datafarm.apgrid.org/ >.
<u>GGF Semantic Grid Research Group</u> and the Semantic Grid Community Portal	Semantic Grid, <i>Semantic Grid Community Portal</i> (2006) < http://www.semanticgrid.org/index.html >.
GSI	Globus Grid Security Infrastructure: The Globus Alliance, <i>About the Globus Alliance</i> (2006) < http://www.globus.org/alliance/about.php >.
Grid Canada	Grid Canada, <i>About GC</i> (2002) < http://www.gridcanada.ca/about.html >.
GridSphere Project	GridSphere Portal Framework, <i>Welcome to the GridSphere Project!</i> (2006) < http://www.gridsphere.org/gridsphere/gridsphere >.
GriddLes	Grid Enabling Legacy Software: GriddLes, <i>Home</i> (2005) < http://www.csse.monash.edu.au/~davidagriddles/ >.
ICTs	Information and communication technologies.
IdP	Shibboleth Identity Provider
IEMSR	JISC IE Metadata Schema Registry Project by ILRT and UKOLN: JISC IE Metadata Schema Registry, <i>Home</i> (2006) < http://www.ukoln.ac.uk/projects/iemsr/ >.
Internet2	Internet2 [®] , <i>About Internet2[®]</i> (2006) < http://www.internet2.edu/about/ >.
IP	Intellectual property. See description above in Glossary of Terms.
JAINIS	JCU And Indiana Instrument Services
JCU	James Cook University.
JISC	Joint Information Systems Committee: Joint Information Systems Committee, <i>About JISC</i> (2006) < http://www.jisc.ac.uk/index.cfm?name=about >.
MAMS	Meta Access Management System Project: Meta Access Management System (MAMS), <i>MAMS Project Overview</i> (2005)

Initials	Full Text
	< http://www.melcoe.mq.edu.au/projects/MAMS/ >.
MCAT	Metadata catalogue: SDSC SRB, <i>MCAT</i> (2006) < http://www.sdsc.edu/srb/index.php/MCAT >.
MERRI	Managed Environments for Research Repository Infrastructure: Department of Education, Science and Training, <i>ARIIC Projects</i> (2005) < http://www.dest.gov.au/sectors/research_sector/policies_issues_reviews/key_issues/australian_research_information_infrastructure_committee/ariic_projects.htm >.
Monash Sun Grid	See: Monash University <i>Monash Sun Grid</i> (2006) < http://www.monash.edu.au/eresearch/activities/msg.html >.
Mosfim	Crystallography analysis software.
MU	Monash University.
National Optical Astronomy Observatory	National Science Foundation, <i>National Optical Astronomy Observatory (NOAO)</i> (2006) < http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=5663 >.
National Radio Astronomy Observatory	National Science Foundation, <i>National Radio Astronomy Observatory (NRAO)</i> (2006) < http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=5653&org=AST&from=home >.
National STEM Education Digital Library	National Science Foundation, <i>National STEM Education Digital Library (NSDL)</i> (2005) < http://www.nsf.gov/ehr/rec/nsdlinks.jsp >.
NCRIS	National Collaborative Research Infrastructure Strategy: Department of Education, Science and Training, <i>National Collaborative Research Infrastructure Strategy, Strategic Roadmap</i> (2006) < http://www.dest.gov.au/sectors/research_sector/policies_issues_reviews/key_issues/ncris/ >.
Nimrod/G	Nimrod, <i>Nimrod/G</i> (2005) < http://www.csse.monash.edu.au/~davida/nimrod/nimrodg.htm >.
NLA	National Library of Australia: National Library of Australia, <i>Home</i> (2006) < http://www.nla.gov.au/ >.
NSF	National Science Foundation: National Science Foundation (2005), <i>NSF-wide investment – Cyberinfrastructure</i> (2006) < http://www.nsf.gov/news/priority_areas/cyberinfr >.

Initials	Full Text
	astructure/index.jsp >.
Ontario Scholars Portal	Scholars Portal, <i>Welcome to Scholars Portal</i> (2005) < http://www.scholarsportal.info/ >.
OntoGrid project	OntoGrid Project, <i>Home</i> (2006) < http://www.ontogrid.net/ontogrid/index.jsp >.
OWL	Web Ontology Language: World Wide Web Consortium, <i>Semantic Web</i> (2006) < http://www.w3.org/2001/sw/ >.
PDB	RCSB Protein Data Bank: RCSB Protein Data Bank, <i>Welcome to the RCSB PDB</i> (2006) < http://www.rcsb.org/pdb/home/home.do >.
PKI	Public Key Infrastructure (see described above in Glossary of Terms, Appendix B).
PORTIA	Privacy, Obligations and Rights in Technologies of Information Assessment: Privacy, Obligations, and Rights in Technologies of Information Assessment, <i>Project Description</i> (2006) < http://crypto.stanford.edu/portia/ >.
R	Relying parties.
RAs	Registration Authorities.
RDF	Resource Description Framework: World Wide Web Consortium, <i>Semantic Web</i> (2006) < http://www.w3.org/2001/sw/ >.
S	Subscribers.
SAML	Security Assertion Markup Language
SC	Science Commons project: Science Commons, <i>Science Commons</i> (2006) < http://sciencecommons.org/ >.
SSL	Secure Sockets Layer.
Semantic Grid	Semantic Grid, <i>Semantic Grid Community Portal</i> (2006) < http://www.semanticgrid.org/ >.
Semantic Web	T Berners-Lee, J Hendler and O Lassila, 'The Semantic Web' (2001) 284 <i>Scientific American</i> 34-43.
SI	Storage and Interoperability (a group of DART work packages).
SII	Systemic Infrastructure Initiative: Department of Education, Science and Training, <i>Systemic</i>

Initials	Full Text
	<i>Infrastructure Initiative (SII)</i> (2005) < http://www.dest.gov.au/sectors/higher_education/programmes_funding/programme_categories/research_related_opportunities/systemic_infrastructure_initiative/ >.
Shibboleth	Internet2®, <i>Shibboleth</i> (2006) < http://shibboleth.internet2.edu/ >.
SP	Shibboleth Service Provider.
SRB	Storage Resource Broker: SRB, <i>Main Page</i> (2006) < http://www.sdsc.edu/srb/index.php/Main_Page >.
SSI	Sea Surface Temperature.
UQ	University of Queensland.
UU	Unauthorised User.
VALET	Visionary Technology in Library Solutions, <i>VALET for ETDs</i> (2006) < http://www.vtls.com/Products/ >.
Vannotea	The University of Queensland Australia, <i>Vannotea</i> (2006) < http://www.itee.uq.edu.au/~eresearch/projects/vannotea/index.html >.
VTLS	Visionary Technology for Library Systems, Inc, see: Visionary Technology for Library Systems, <i>Home</i> (2006) < http://www.vtls.com/ >.
Web 2.0	T O'Reilly, 'What Is Web 2.0?: Design Patterns and Business Models for the Next Generation of Software' (2005) < http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html >.
WSIS	World Summit on the Information Society: World Summit on the Information Society, <i>Geneva Declaration of Principles</i> , principles A2 and A7, Document WSIS-03/GENEVA/DOC/4-E (2003) < http://www.itu.int/wsis/docs/geneva/official/dop.html >; World Summit on the Information Society, <i>Tunis Commitment</i> , principles 9 and 10, Document: WSIS-05/TUNIS/DOC/7- 18 November 2005 (2005) < http://www.itu.int/wsis/docs2/tunis/off/7.html >.
WWW	World Wide Web.
W3C	World Wide Web Consortium: World Wide Web Consortium, <i>About the World Wide Web Consortium (W3C)</i> (2006) < http://www.w3.org/Consortium/ >.

Initials	Full Text
XML	Extensible Markup Language.