

## e-RESEARCH AND JURISDICTION

**Gaye Middleton<sup>1</sup>**

As part of their daily activities, those involved in e-research will often transfer information, including background materials, research results and software, across state and national borders. The act of transferring information across state and national borders raises a number of jurisdictional issues. This chapter will discuss key issues regarding intellectual property, privacy and dispute resolution as they arise from e-researchers transferring information across state and national borders, and how these issues may contractually be resolved.

### INTELLECTUAL PROPERTY ISSUES

There are two key jurisdictional issues relating to intellectual property rights which are raised by the transfer of information across state and national borders. These are:

- the differing intellectual property protection available in different jurisdictions; and
- the possibility that the transfer of information or materials from one jurisdiction to another may result in intellectual property infringement in the recipient jurisdiction.

These jurisdictional issues arise because intellectual property rights are territorial rights, as they are created by national laws that, subject to certain limited exceptions, only apply within the boundaries of the nation which passed those laws.

---

<sup>1</sup> Inhouse Counsel, Uecomm Operations Pty Ltd.

## Differing Intellectual Property Protection

E-researchers engaged in cross-border research projects may be affected by jurisdictional differences in the protection afforded to intellectual property rights.

There are numerous international treaties, such as the *Berne Convention for the Protection of Literary and Artistic Works* and the *Agreement on Trade Related Aspects of Intellectual Property (TRIPS)*, which require the signatories to enact intellectual property laws which comply with the standards laid down by those treaties.<sup>2</sup> However, even as between member states to these treaties, intellectual property laws are not uniform. Factors which contribute to this lack of uniformity between intellectual property laws in countries which are member states of the same international treaties include:

- differences in the wording of intellectual property legislation between those member states; and
- differences in the way in which those treaties and the implementing legislation is interpreted by the courts of those member states.

For example, in Australia, an author is entitled to copyright protection for a work that the author has created if it originated from the author in that it was not copied, and the author expended skill, labour or expense in creating that work.<sup>3</sup> No degree of inventiveness or originality is needed to obtain copyright protection for a work in Australia. This means that a compilation of unoriginal facts or figures may be protected by copyright in Australia if the author can show that labour, skill or expense were used in making that compilation.<sup>4</sup> By contrast, in the United States, both labour and creativity are required to obtain copyright

---

<sup>2</sup> See generally A Fitzgerald and B Fitzgerald, *Intellectual Property in Principle* (2004).

<sup>3</sup> *University of London Press Ltd v University Tutorial Press Ltd* [1916] 2 Ch 601, 601–9 (Joyce J); *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 479, 498 (Latham CJ), 511 (Dixon J); *Desktop Marketing Systems Pty Ltd v Telstra Corporation Limited* [2002] FCAFC 112, [160]; *Nine Network Australia Pty Ltd v Ice TV Pty Ltd* [2008] FCAFC 71.

<sup>4</sup> *Ladbroke (Football) Ltd v William Hill (Football) Ltd* [1964] 1 WLR 273 (HL), 285 (Lord Hodson), 289 (Lord Devlin); *Computer Edge Pty Ltd v Apple Computer Inc* (1986) 161 CLR 171, 182–3 (Gibbs CJ); *Desktop Marketing Systems Pty Ltd v Telstra Corporation Limited* [2002] FCAFC 112, [160].

protection for a work.<sup>5</sup> This means that works such as a database of facts and figures compiled by researchers may be protected by copyright in Australia, but when that database is transferred by researchers to another jurisdiction, such as the United States, it may not be protected by copyright.

Further, the duration of copyright protection varies between nations. As a result of the implementation of the *Australia – United States Fair Trade Agreement*,<sup>6</sup> Australia and the United States both provide general copyright protection in works for the life of the author plus 70 years after the author's death.<sup>7</sup> By contrast, in Japan, the term of general copyright protection in works is currently life plus 50 years.<sup>8</sup> This means that works that are no longer protected by copyright and hence are able to be used freely by researchers in one jurisdiction may remain subject to copyright protection in another jurisdiction. For example, if researchers in a multi-jurisdictional research collaboration need to use the same work, the researchers in one jurisdiction may be able to do so without restriction, while the researchers in another jurisdiction may have to obtain a licence of that work for the purposes of their research.

### Transfer of Information and Intellectual Property Infringement

Another jurisdictional issue relating to intellectual property rights which faces e-researchers is that, due to the differences in intellectual property laws between countries, the transfer of information or materials from one country to another may, in certain circumstances, result in intellectual property infringement in the recipient jurisdiction. This infringement may occur even though the use of the transferred information or materials in the originating jurisdiction does not infringe the intellectual property rights of others. The reason for this is that, although intellectual property rights are territorial in nature, there are certain circumstances in which the intellectual property laws of a country

---

<sup>5</sup> *Feist Publications, Inc v Rural Telephone Service Co Inc* 499 US 340 (1991).

<sup>6</sup> For a copy of the Free Trade Agreement and associated documents, see: <[http://www.dfat.gov.au/trade/negotiations/us\\_fta/final-text/index.html](http://www.dfat.gov.au/trade/negotiations/us_fta/final-text/index.html)> at 16 January 2007.

<sup>7</sup> *Australia - United States Free Trade Agreement 2004* art 17.4.4; *Copyright Act 1968* (Cth).s 33.

<sup>8</sup> *Japanese Copyright Act* art 51.

can apply extraterritorially. This means that acts done outside of that country may infringe the intellectual property laws of that country.

One example of the extraterritorial application of Australian copyright law is liability for authorisation infringement. A person who uploads a work protected by Australian copyright onto the Internet outside Australia without the author's authority could be liable for authorising infringement of copyright in that work within Australia if an infringing copy of that work is made in Australia from the unauthorised copy that was uploaded onto the Internet outside of Australia. This is because, if a person authorises an infringing act by another person that takes place within Australia, it does not matter for the purposes of section 36 of the *Copyright Act 1968* (Cth), which deals with authorisation infringement, that the first person authorised the infringement outside of Australia. The fact that the infringing act which that person authorised takes place in Australia is sufficient to establish liability for authorisation infringement.<sup>9</sup>

Some United States courts have applied United States copyright laws outside of the United States by applying a principle known as the 'root copy' doctrine. Under the root copy doctrine, a person may be liable for infringement of US copyright in respect of a work where that person makes an unauthorised copy of a work protected by copyright in the United States, not only for making the unauthorised copy itself, but also for any distribution of that infringing copy outside of the United States.<sup>10</sup> An example of the potential application of the root copy doctrine in the context of e-research is where a researcher in the United States makes an unauthorised copy of research results that are protected by copyright, and provides that copy to his or her colleagues in Australia, where it is further distributed. In these circumstances, the researcher based in the United States may be liable for copyright infringement both for making the initial copy and for its distribution outside of the United States.

---

<sup>9</sup> S Ricketson and C Creswell, *The Law of Intellectual Property: Copyright, Designs and Confidential Information* (2002) [16A.145].

<sup>10</sup> *Update Art v Modii Publishing Ltd* 843 F 2d 67, 82 (2nd Cir 1988). See further discussion of this doctrine in G Austin, *Private International Law and Intellectual Property Rights – A Common Law Overview* (WIPO, 2001) [31] <[http://www.wipo.int/edocs/mdocs/mdocs/en/wipo\\_pil\\_01/wipo\\_pil\\_01\\_5.pdf](http://www.wipo.int/edocs/mdocs/mdocs/en/wipo_pil_01/wipo_pil_01_5.pdf)> at 12 January 2007.

In respect of patents, a person in Australia who electronically uses an Australian patented invention hosted by a foreign person on a server situated outside Australia, or who imports data generated by that invention into Australia via the internet, may infringe the Australian patent for that invention. However, the person who operates the website from which the invention is accessed may also be liable for contributory patent infringement under section 117 of the Australian *Patents Act* for supplying a product, in this case, being data or information, which infringes an Australian patent.<sup>11</sup>

E-researchers may infringe United States patent laws by acts done outside of the United States under section 271(f) of the United States *Patent Act* by supplying in or from the United States, without the patent holder's authority, all or a substantial number of the unassembled components of a patented invention so as to actively induce the combination of those components outside the United States in a way which would infringe the patent for that invention if those components were combined within the United States.

A recent series of cases in the United States considers whether software source code is a component of a patented invention such that, if a person supplies that source code to others outside of the United States, and thereby enables the conduct of foreign activities that would have infringed copyright in the relevant invention in the United States, then the supplier is liable for inducement infringement under section 271(f) of the United States *Patent Act*.

In the first of this series of cases, *Eolas Technologies Inc v Microsoft Corp*,<sup>12</sup> the Court of Appeals for the Federal Circuit held that Microsoft was liable for inducement infringement of an Eolas patent when it shipped master disks containing source code for its Internet Explorer® computer program to hardware manufacturers outside of the United States, who then used those master disks to load Internet Explorer® directly onto their hardware. The Court held that source code can be a

---

<sup>11</sup> J Swinson and G Middleton, 'The effectiveness of patent protection for e-commerce technologies' (Proceedings of the Technology Transfer and Innovation Conference 2001, Brisbane, 2001). This area of patent law is still uncertain, as is the application of *Patents Act 1990* (Cth) s 117. For a summary of decisions regarding the operation of the *Patents Act* s 117, see commentary in J Lahore et al, *Patents, Trade Marks and Related Rights* (Butterworths, subscription service) [18,285].

<sup>12</sup> 399 F 3d 1325 (Fed Cir 2005).

component of a computer program invention for the purposes of section 271(f) of the US *Patent Act*, even though:

- neither source code nor a computer program is a physical object; and
- the content of the master disks was copied onto hardware and the disks themselves did not form part of the final product.

By contrast, in *Microsoft Corporation v AT&T*,<sup>13</sup> the Supreme Court of the United States found that Microsoft was not liable for inducement infringement under section 271(f) of the US *Patent Act* where Microsoft supplied master disks for its Windows® computer program to manufacturers outside of the United States, and those foreign manufacturers loaded the content from copies of the master disks onto their foreign-made hardware, rather than from the master disks themselves. As Microsoft had not supplied the foreign-made copies of the master disks that the foreign manufacturers combined with their hardware to form AT&T's patented invention, the court found that Microsoft did not supply components of AT&T's patented invention from the United States which were combined to make the patented invention outside of the United States.

These cases are relevant to researchers who electronically distribute software source code from the United States to colleagues in another jurisdiction. They demonstrate that supplying source code which constitutes a 'component' of a patented invention to a person outside of the United States may result in a researcher inadvertently infringing a United States patent.

## PRIVACY

Privacy has been defined as the claim of individuals, groups or institutions to determine when, how and to what extent information about them may be communicated to others.<sup>14</sup> There are various categories of privacy, including bodily privacy, privacy of

---

<sup>13</sup> US Supreme Court, No. 05–1056, 30 April 2007, overturning the decision of the Court of Appeals for the Federal Circuit in *AT&T v Microsoft Corporation* 414 F 3d 1366 (Fed Cir 2005).

<sup>14</sup> A F Westin, *Privacy and Freedom* (1967) 7.

communications and territorial privacy.<sup>15</sup> However, in this chapter, the term ‘privacy’ refers solely to information privacy, being the rules which govern the collection and handling of personal information. ‘Personal information’ is defined in section 6 of the Australian *Privacy Act 1988* (Cth) as:

Information or an opinion ... whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Within Australia, e-researchers may be bound, not only by the Commonwealth *Privacy Act*, but also by state and territory laws dealing with privacy. While the state and territory privacy legislation is similar to the Commonwealth privacy legislation, there are certain differences. This may raise jurisdictional issues when information is transferred within Australia between researchers situated in different States and Territories. For example, in respect of personal information concerning deceased persons, the Commonwealth *Privacy Act* only applies to persons who are alive, as does the Victorian *Information Privacy Act 2000*. However, under the Northern Territory’s *Information Act 2002*, information about a person continues to be protected for 5 years after their death; in Tasmania, under the *Personal Information Protection Act 2004*, personal information is protected until 25 years after a person’s death; and under the New South Wales *Privacy and Personal Information Protection Act 1998*, personal information is protected for 30 years after a person’s death.<sup>16</sup> Accordingly, even within Australia, researchers must take care to comply with the privacy legislation in each state or territory where that information is transferred.

The Commonwealth *Privacy Act* imposes restrictions on the transborder flow of data under the National Privacy Principles. The National

---

<sup>15</sup> B Fitzgerald, A Fitzgerald, G Middleton, YF Lim and T Beale, *Internet and E-commerce Law: Technology, Law and Policy* (2007) [10.10], citing D Banisar, *Privacy and Human Rights 2000: An International Survey of Privacy Law and Developments* (Electronic Privacy Centre and Privacy International) <<http://privacyinternational.org/survey/phr2000/overview.html>> at 14 May 2007.

<sup>16</sup> D Lindsay, A Monotti, M Paterson and A Chin, *Legal Issues in eResearch: Report for the Content and Rights Work Package (CR6) – Dataset Acquisition, Accessibility and Annotation e-Research Technologies Project* (2006) 101, Table 5.2 <<http://www.dart.edu.au/workpackages/cr/cr6.html>> at 29 July 2007.

Privacy Principles ('NPPs') primarily apply to researchers in private sector organisations with an annual turnover of more than \$3 million per annum or researchers working for health service providers.<sup>17</sup> This means that researchers in the public sector (that is, government) or in the majority of universities, which are established under State law rather than Commonwealth law, will not be bound by the NPPs.<sup>18</sup> Under NPP 9 in Schedule 3 of that Act, an organisation may not transfer personal information to someone in a foreign country that does not have a comparable information privacy scheme to Australia, unless the individual whose personal information is being disclosed consents to that transfer, or where, among other things:

- the organisation reasonably believes that the recipient of the information is subject to a law or other instrument which requires the recipient to handle personal information in a similar way to the National Privacy Principles; or
- the transfer benefits the individual, and is necessary for the performance of a contract between the individual and the organisation; or
- the transfer benefits the individual, and while the individual's consent cannot be obtained, the transferring organisation can show grounds for the belief that the individual would give their consent if it were possible to obtain it; or
- the organisation has taken reasonable steps to ensure that personal information that it transfers will not be held, used or disclosed by the recipient in a manner which is inconsistent with the National Privacy Principles.

However, NPP9 does not prevent the transfer of personal information outside of Australia by an organisation to:

---

<sup>17</sup> *Privacy Act 1988* (Cth) s 16A. See also A Hayne, 'Privacy Regulation and e-Research' (Paper presented at the Legal Framework for e-Research Conference, Gold Coast Queensland, 11–12 July 2007) 4 at <[http://www.privacy.gov.au/news/speeches/spp07\\_07.pdf](http://www.privacy.gov.au/news/speeches/spp07_07.pdf)> at 24 June 2008.

<sup>18</sup> The privacy obligations of Commonwealth government departments and agencies are set out in the Information Privacy Principles ('IPPs') in section 14 of the *Privacy Act 1988* (Cth). The IPPs do not contain specific provisions restricting transborder data flows. Researchers in universities and institutions established under State law are subject to the privacy legislation in the relevant State. Most States which have legislative privacy principles have based them on the Commonwealth IPPs, hence they also do not contain specific provisions restricting transborder data flows.



- another part of the same organisation; or
- the individual to whom that information relates.

NPP 9 is based on the restrictions on cross-border transfers of personal information laid down by European Commission Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data ('Directive'). Article 25 of the Directive prohibits the transfer of personal data to countries which do not provide adequate levels of data privacy. The European Union ('EU') does not yet recognise Australian privacy laws as adequate for this purpose. One reason for this is that NPP 9 permits the transfer of personal information across national borders where the transferring organisation 'reasonably believes' that the recipient is bound by a law or other instrument which is substantially similar to the National Privacy Principles; by contrast the Directive requires that the recipient *must* be in a country with an adequate level of protection. Another reason why the EU does not recognise Australian privacy laws as adequate for the purposes of the Directive is that it permits an organisation to transfer personal information across national borders where it has simply taken 'reasonable steps' to ensure that the recipient will not deal with that information inconsistently with the National Privacy Principles. This exception is regarded as weak and imprecise.<sup>19</sup>

Where personal information is transferred across national boundaries, the differences in privacy laws become significant, making compliance with those laws difficult. To add to the complexity, the United States does not have a single piece of legislation which comprehensively regulates information privacy in the private sector. Instead, information privacy is regulated by a patchwork of sector-specific legislation, the tort of invasion of privacy and trade practices legislation.<sup>20</sup>

---

<sup>19</sup> Office of the Privacy Commissioner, *Issues Paper – Review of the private sector provisions of the Commonwealth Privacy Act 1988* (Australian Government, Canberra, 2004) 22–3 <<http://www.privacy.gov.au/act/review/ispap2004.pdf>> at 29 July 2007; Australian Law Reform Commission, *Issues Paper 31 - Review of Privacy* (Australian Law Reform Commission, 2006) [13.59]–[13.72] <<http://www.austlii.edu.au/au/other/alrc/publications/issues/31/>> at 29 July 2007.

<sup>20</sup> For example, see J Reidenberg, 'Privacy Wrongs in Search of Remedies' (2003) 54 *Hastings LJ* 877, 880–1.

Even between EU countries, there is a wide degree of variance in data privacy laws. This arises primarily because of the different ways in which data privacy is protected in the member states. Some countries, such as Portugal and Spain, have enacted specific data protection provisions in their constitutions. Other countries derive data protection from their existing constitutional principles without specifically referring to data protection. For example, Germany derives the right to data privacy from the general right to respect for one's personality. In the United Kingdom, which does not have a written constitution, the right to data privacy is derived from certain rights in the European Convention on Human Rights, which is incorporated into its national laws.<sup>21</sup>

Because of the wide variations in privacy laws between jurisdictions, it can be a compliance nightmare for researchers who transfer personal information across national borders. The Directive regulating privacy in the EU currently sets the highest standard for information privacy; accordingly, if researchers take steps to comply with the Directive in respect of the transfer of personal information across national borders, then they will be likely to have satisfied the privacy laws of most jurisdictions.

## DISPUTE RESOLUTION ISSUES

If a dispute arises between researchers in different states, territories or countries, there are two key jurisdictional issues which arise. These issues are:

- first, which courts have the authority to require the parties to the dispute to appear before it for the purposes of deciding the dispute; and
- second, which country's laws should be applied to determine the dispute.

---

<sup>21</sup> D Korff, *EC Study on Implementation of Data Protection Directive – Comparative Study of National Laws* (Human Rights Centre, 2002) 8–9  
<[http://ec.europa.eu/justice\\_home/fsj/privacy/docs/lawreport/consultation/univessex-comparativestudy\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/consultation/univessex-comparativestudy_en.pdf)>.

## Personal Jurisdiction

If a court has authority to require a person to appear before it in respect of a dispute, that court is said to have personal jurisdiction over that person.

At common law, for a court to have personal jurisdiction over a person, that person must be served with court proceedings while that person is physically within that court's geographical jurisdiction.<sup>22</sup> Under Australian law, there are limited circumstances in which a person may be served with court proceedings when they are outside the court's geographical jurisdiction. These circumstances, which are governed by the rules of that court, include:

- where the dispute concerns a contract which was made or broken within the jurisdiction, or which is governed by the laws of that jurisdiction;
- where the dispute concerns a tortious act committed within the jurisdiction; or
- where the dispute concerns a breach of legislation which took place within the jurisdiction.<sup>23</sup>

This means that a researcher involved in a multi-jurisdictional research project who communicates with the other participants in the research project entirely by electronic means may be subject to court proceedings in another state or country, even if that researcher has never physically entered that state or country.

## Choice of Law

Where a court has personal jurisdiction over the parties to a dispute, but where more than one forum has a connection with the dispute, the court must decide which forum's laws it will apply to decide the dispute. To decide which forum's laws it will apply in these circumstances, a court

---

<sup>22</sup> *Laurie v Carroll* (1958) 98 CLR 310.

<sup>23</sup> For a discussion of the circumstances in which a person may be served with proceedings when they are physically outside the jurisdiction of a court, see P Nygh and M Davies, *Conflict of Laws in Australia* (7th ed, 2002) 51–75; Butterworths, *Halsbury's Laws of Australia*, 85 Conflict of Laws [85–335]ff; Law Book Company, *The Laws of Australia*, 5 Civil Procedure [4]ff; B Fitzgerald, A Fitzgerald, G Middleton, YF Lim and T Beale *Internet and e-commerce law: technology, law and policy* (2007), n13 at [2.40]–[2.60].

will use what are known as ‘choice of law’ rules. Accordingly, those involved in e-research may not only be subject to court proceedings in a place other than their home state or country, but they may also be subject to the laws of another state or country in respect of those proceedings.

Different choice of law rules apply to different categories of dispute. In respect of contractual disputes, if there is no governing law clause or other choice of law which can be implied from the contract itself, then Australian courts will apply the law with which the contract has the closest and real connection at the time it is formed.<sup>24</sup> Factors relevant to determining which forum’s laws should apply in respect of a contract dispute include the form and legal language of the contract, the place where the contract is made, the place where the contract is to be performed and the place of residence of the parties to the contract. By contrast, Australian courts will apply the law of the place of the wrong, known as the ‘lex locus delicti’, when deciding disputes concerning tortious acts, such as negligence or defamation.<sup>25</sup>

## CONTRACT AS A MEANS OF RESOLVING JURISDICTIONAL ISSUES

The jurisdictional issues confronting e-researchers that are discussed in this chapter can be addressed by a research collaboration agreement between the researchers who are working together on an e-research project.<sup>26</sup>

Jurisdictional issues which can be dealt with by e-researchers in a research collaboration agreement include the following:

- The agreement may state the laws of the forum which will apply when interpreting and administering that agreement.<sup>27</sup>

---

<sup>24</sup> *Oceanic Sun Line Special Shipping Co Inc v Fay* (1988) 165 CLR 197, 217.

<sup>25</sup> *John Pfeiffer Pty Ltd v Rogerson* (2000) 203 CLR 503; *Regie National des Usines Renault SA v Zhang* (2002) 210 CLR 491.

<sup>26</sup> B Fitzgerald and J Abbot, *Legal Framework for e-Research* (2006) 3 <[http://eprints.qut.edu.au/archive/00005311/01/5311\\_1.pdf](http://eprints.qut.edu.au/archive/00005311/01/5311_1.pdf)>.

<sup>27</sup> For limits on this approach see B Fitzgerald, A Fitzgerald, G Middleton, YF Lim and T Beale, *Internet and e-commerce law: technology, law and policy* (2007) [2.200], [2.230]. See also *Bragg v Linden Research, Inc and Rosedale* 487 F. Supp. 2d 593 (E.D. Pa. 2007), where Robreno J of the US District Court for the Eastern District of Pennsylvania rejected the defendant’s motion to

- The agreement may state the courts of the forum which will have power to decide disputes arising in respect of the research project.<sup>28</sup>
- The agreement may state how intellectual property rights developed during the course of the research project will be owned and how they may be dealt with by the participants in the project.<sup>29</sup>
- The agreement may state the privacy obligations of each party to the research collaboration.<sup>30</sup>

---

dismiss the plaintiff's action brought in that court and the defendant's motion to compel arbitration. The defendant's motions cited, among other things, its Terms of Service for using Second Life, its online virtual world. These Terms of Service included a choice of law and jurisdiction clause which stated that the laws of California governed the contract between the parties, and that all disputes would be settled by binding arbitration in San Francisco, California, according to the rules of the International Chamber of Commerce. In registering to use Second Life, the plaintiff agreed to these Terms of Service. However, Robreno J held (at page 611) of the judgment that the choice of law and jurisdiction clause was not enforceable against the plaintiff because:

Taken together, the lack of mutuality, the costs of arbitration, the forum selection clause, and the confidentiality provision that Linden unilaterally imposes through the [Terms of Service] demonstrate that the arbitration clause is not designed to provide Second Life participants an effective means of resolving disputes with Linden. Rather, it is a one-sided means which tilts unfairly, in almost all situations, in Linden's favor.

<sup>28</sup> For limits on this approach see B Fitzgerald, A Fitzgerald, G Middleton, YF Lim and T Beale, *Internet and e-commerce law: technology, law and policy* (2007) [2.70], [2.85]-[2.90]. See also the discussion regarding *Bragg v Linden Research, Inc and Rosedale* 487 F. Supp. 2d 593 (E.D. Pa. 2007) at footnote 27 above.

<sup>29</sup> However, where researchers develop intellectual property based on a third party's pre-existing intellectual property, the terms of the licence to use that intellectual property may stipulate who owns any intellectual property developed from the licensed intellectual property. For example, it is common for licensors of intellectual property to stipulate as a licence condition that any modifications or improvements to the licensed intellectual property developed by licensees will be owned by the licensor.

<sup>30</sup> The terms of a research collaboration agreement cannot override legislative privacy obligations. However, contractual privacy provisions can serve to make participants in an e-research project aware of their statutory privacy obligations, and may also serve as a means to obtain consent from the participants in a research project to the use of their own personal information for the purposes of that project.

A research collaboration agreement which deals with these issues is an important tool for researchers to minimise their potential legal risk. However, a research collaboration agreement is not the only source of their rights and obligations in respect of these issues, and it is vital for e-researchers to take account of other sources of these rights and obligations which may impact on their research project. In addition to statutory rights and obligations, there may, for example, be licences applicable to certain materials used in the research project. These materials may be licensed by traditional intellectual property licences, or be subject to an open access licence. Ideally, e-researchers should identify these other sources of rights and obligations prior to drafting a research collaboration agreement in respect of their research project so that the terms of that agreement are consistent with and subject to those other sources.

## CONCLUSION

This chapter discusses key jurisdictional issues which arise from the transfer of research information across state and national boundaries in the conduct of e-research. To minimise their legal exposure resulting from these jurisdictional issues, it is important for e-researchers to enter into a research collaboration agreement which adequately addresses each of these issues. Such an agreement cannot provide e-researchers with an absolute solution to complex jurisdictional issues, given the multiple sources of rights and obligations which may impact on a research project. However, it enables the parties to a multi-jurisdictional research project to better understand the legal obligations that apply to them as a result of transferring information across national boundaries, and to provide themselves with some degree of certainty regarding the applicable laws and forum if a dispute arises between them at a later stage.